FortiClient v5.0
Administration Guide

FortiClient v5.0 Administration Guide

January 09, 2013

04-501-183401-20130109

Copyright© 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log **6**

Introduction **7**

Licensing 7

Client limits 7

Supported operating systems 8

Windows 8

Mac OS X 8

Minimum system requirements 8

Windows 8

Mac OS X 8

Language support 9

Windows 9

Mac OS X 9

What's New in FortiClient v5.0 ..... **10**

Summary of enhancements 10

Installing FortiClient **12**

Installing FortiClient on a Windows computer 12

Installing FortiClient on a Mac OS X computer 15

Provisioning FortiClient **18**

FortiClient MSI configuration tool 18

Usage 18

Example usage 18

FortiClient Configurator application 18

Creating a custom MSI installation file 19

Deploy FortiClient using Microsoft Active Directory (AD) server 19

Deploy using Microsoft System Center Configuration Manager 2007 20

Endpoint Management **23**

Introduction 23

Configure Endpoint Management 23

Step 1: Enable Device Management and Broadcast Discovery Messages 23

Step 2: Configure the Client Endpoint Profile 24

Step 3: Configure Firewall Policies 25

Step 1: Download and install FortiClient 28

Step 2: FortiClient registration 28

Step 3: FortiGate deploys the Endpoint Profile 30

Deploy the Endpoint Profile to clients over VPN 31

Remembered FortiGates 32

View FortiClient registration on the FortiGate Web-based Manager 33

Configure preferred FortiGate IP on FortiClient for registration 34
Enable FortiClient Endpoint Registration (optional) 34
Antivirus 35
FortiClient Antivirus 35
Enable/Disable Antivirus 35
Notifications 35
Scan Now 36
Scan a file or folder 37
Update Now 37
Schedule Antivirus scanning 38
View quarantined threats 39
Add files/folders to an exclusion list 40
Antivirus warning 40
Antivirus logging 41
Antivirus options 42
Parental Control/Web Filtering 43
FortiClient Parental Control/Web Filtering 43
Enable/Disable Parental Control/Web Filtering 43
Parental Control/Web Filtering settings 44
View profile violations 44
Application Firewall 45
FortiClient Application Firewall 45
Enable/Disable Application Firewall 45
View Applications blocked 45
Application Firewall rules 46
Application Firewall logging 47
IPsec VPN and SSL-VPN 48
FortiClient Remote Access (VPN) 48
Add a new connection 48
Create a new SSL-VPN connection 48
Create a new IPsec VPN connection 50
Connect to a VPN 51
Advanced features (Windows) 52
Connect VPN before logon (AD environments) 52
Create a redundant IPsec VPN 53
Priority based SSL-VPN connections 53
Enabling VPN autoconnect 54
Enabling VPN always up 54

Advanced features (Mac OS X) 55
Create a redundant IPsec VPN 55
Priority based SSL-VPN connections 55
For SSL-VPN, all FortiGates must use the same TCP port. 56
Enabling VPN autoconnect 56
Enabling VPN always up 56
VPN tunnel & script (Windows) 56
Feature overview 56
Map a network drive after tunnel connection 57
Delete a network drive after tunnel is disconnected 57
VPN tunnel & script (Mac OS X) 57
Map a network drive after tunnel connection 57
Delete a network drive after tunnel is disconnected 58
Vulnerability Scan 59
Vulnerability Scan 59
Scan Now 59
Update Now 59
View Vulnerabilities 60
Vulnerability Scan logging 61
Settings 62
Backup or restore full configuration 62
Logging 63
Updates 63
VPN options 64
Certificate Management 64
Antivirus options 64
Advanced options 65
Single Sign-On Mobility Agent 66
FortiClient/FortiAuthenticator Protocol 66
Configuration lock 68
FortiTray 69
Connect to a VPN connection 70
Index 71

Change Log

Date	Change Description
2012-11-02	Initial release.
2012-11-07	Updated scripts chapters. This document is now inclusive of both Windows and Mac OS X. It is important to note that not all features available for Windows are available for Mac OS X.
2012-11-15	Updated IPsec and SSL-VPN chapter.
2012-11-22	Added note about FortiClient License for FortiAuthenticator.
2012-11-27	Updated script commands to match changes in the *FortiClient v5.0 XML Reference*.
2013-01-09	Updated for FortiClient v5.0 Patch Release 1. Removed XML chapter, see to the *FortiClient v5.0 XML Reference* for more information. Removed FortiClient Tools chapter, see the *FortiClient v5.0 Patch Release 1 Release Notes* for more information.

Introduction

FortiClient has been completely re-designed for v5.0. FortiClient provides a comprehensive network security solution for endpoints while improving your visibility and control. FortiClient allows you to manage the security of multiple endpoint devices from the FortiGate interface. This document provides an overview of FortiClient v5.0.

This document was written for FortiClient v5.0 Patch Release 1 for Windows. Not all features described in this document are supported for FortiClient v5.0 Patch Release 1 for Mac OS X.

Licensing

Licensing on the FortiGate is based on the number of registered clients. FortiGate 40C and higher models support ten (10) free managed FortiClient licenses. For additional managed clients, an upgraded license must be purchased. The maximum number of managed clients varies per device model.

Client limits

FortiGate Model	Free registrations	FortiClient license upgrade SKU
FortiGate 40, 60, 80 series, VM00	10	N/A
FortiGate 100, 200, 300, 600, 800 series, VM01/VM01-Xen, VM02/VM02-Xen	10	1,000 client registrations FCC-C0103-LIC
FortiGate 1000, 3000, 5000 series, VM04/VM04-Xen, VM08/VM08-Xen	10	3,000 client registrations FCC-C0105-LIC

In high availability (HA) configurations, all cluster members require an upgrade license key.

For more information, go to www.forticlient.com.

Supported operating systems

Windows

- Microsoft Windows 8 (32-bit and 64-bit)
- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows Vista (32-bit and 64-bit)
- Microsoft Windows XP (32-bit)

Mac OS X

- Mac OS X v10.8 Mountain Lion
- Mac OS X v10.7 Lion
- Mac OS X v10.6 Snow Leopard

Minimum system requirements

Windows

- Microsoft Internet Explorer 8.0 or later
- Windows compatible computer with Pentium processor or equivalent
- Compatible operating system and minimum RAM: 512MB
- 600 MB free hard disk space
- Native Microsoft TCP/IP communication protocol
- Native Microsoft PPP dialer for dial-up connections
- Ethernet NIC for network connections
- Wireless adapter for wireless network connections
- Adobe Acrobat Reader or another PDF reader for user manual
- MSI installer 3.0 or later

Mac OS X

- Intel processor
- 256MB of RAM
- 20MB of hard disk drive (HDD) space
- TCP/IP communication protocol
- Ethernet NIC for network connections
- Wireless adapter for wireless network connections

Language support

Windows

FortiClient v5.0 (Windows) is localized for the following languages:

	Graphical User Interface	Documentation
English (United States)	✔	✔
French	✔	-
German	✔	-
Portuguese (Brazil)	✔	-
Spanish (Spain)	✔	-
Chinese (Simplified)	✔	-
Chinese (Traditional)	✔	-
Japanese	✔	-
Korean	✔	-

Mac OS X

FortiClient v5.0 (Mac OS X) is localized for the following languages:

	Graphical User Interface	Documentation
English (United States)	✔	✔
French	✔	-
German	✔	-
Portuguese (Brazil)	✔	-
Spanish (Spain)	✔	-
Chinese (Simplified)	✔	-
Chinese (Traditional)	✔	-
Japanese	✔	-
Korean	✔	-

Please review the *FortiClient v5.0 Patch Release 1 (Windows) Release Notes* or the *FortiClient v5.0 Patch Release 1 (Mac OS X) Release Notes* prior to upgrading. Release Notes are available at the Customer Service & Support site.

What's New in FortiClient v5.0

Summary of enhancements

This document was written for FortiClient v5.0 Patch Release 1 for Windows. Not all features described in this document are supported for FortiClient v5.0 Patch Release 1 for Mac OS X.

The following is a list of enhancements in FortiClient v5.0 (including Patch Release 1):

- Antivirus and Antimalware
  Protection against the latest virus and grayware (adware/riskware) threats.
  Client antivirus is free and auto updates every three hours.
- Application Firewall
  Block, allow, and monitor applications that send traffic to the network.
- Bring Your Own Device (BYOD)
- Diagnostic Tool
- Enhancements to the FortiClient Console
- Endpoint Management using FortiGate, including:
  Automatic endpoint registration and user initiated endpoint registration.
  Deploy VPN (IPsec/SSL) configuration.
  Enable/disable Antivirus real-time protection.
  Manage/deploy Web Filtering and Application Firewall configuration.
  Registration over IPsec VPN or SSL-VPN.
- FortiGuard Analytics
  Automatically send suspicious files to the FortiGuard Network for analysis.
- Localization Support
- Parental Control/Web Filter
  Block, allow, warn, and monitor web traffic based on categories.
- Remember multiple FortiGates for Endpoint Control registrations.
- Remote Access (IPsec and SSL VPN)
  Secure Virtual Private Network (VPN) access to your network.
  Supports multiple gateways for a single tunnel.
- Rootkit detection and removal
- Single Sign-On Mobility Agent support with FortiAuthenticator/FSSO Collector Agent
- Support automatic executing of a custom batch script via an IPsec VPN tunnel
- Support multiple (maximum 10) gateway IP/FQDN in a single IPsec VPN configuration
- Support XML configuration
- VPN from system tray

- VPN auto connect/always up
  Support ability to automatically connect to a VPN tunnel without user interaction.
  Support ability to configure the VPN to always be connected.
- Vulnerability Scan
  Identify system and application vulnerabilities.

Installing FortiClient

Installing FortiClient on a Windows computer

The following instructions will guide you though the installation of FortiClient on a Windows computer.

To install FortiClient

1. Double-click the FortiClient executable file to launch the setup wizard. The *Setup Wizard* will install FortiClient on your computer.

   Figure 1: Welcome screen

Welcome to the FortiClient Setup Wizard
The Setup Wizard will install FortiClient on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Yes, I have read and accept the
License Agreement
Next
Cancel

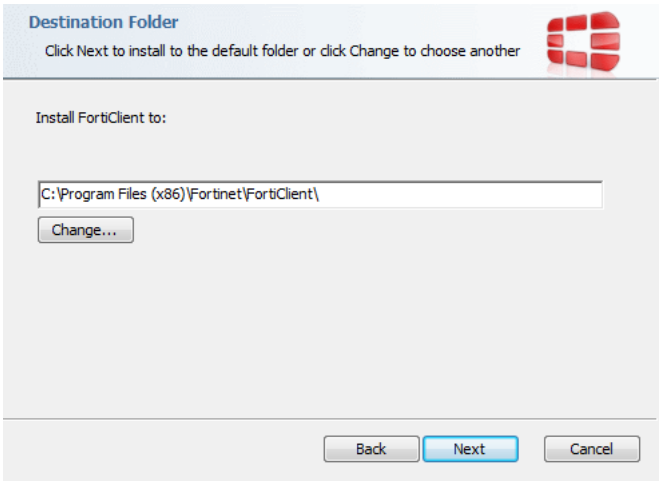
2. Read the license agreement and select *Next* to continue. You have the option to print the EULA on this screen.

   Figure 2: End-User License Agreement

End-User License Agreement
Please read the following license agreement carefully
Fortinet Product License Agreement / EULA and Warranty Terms
Trademarks and Copyright Statement
Fortinet®, FortiGate®, and FortiGuard® are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks, registered or otherwise, of Fortinet. All other product or company names may be trademarks of their respective owners. Copyright © 2002-2011 Fortinet, Inc., All Rights reserved. Contents and terms are subject to change by Fortinet without prior notice. No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet, Inc., as stipulated by the United States Copyright Act of 1976.
Product License Agreement
Print
Close

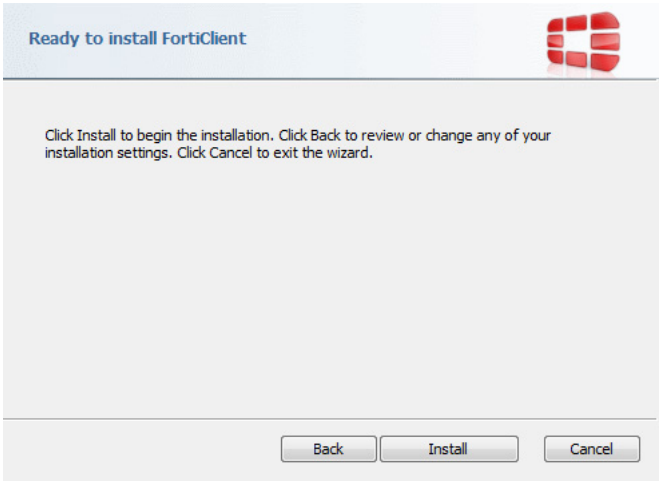
3. Select *Change* to choose an alternate folder destination for installation. Select *Next* to continue.

Figure 3: Destination Folder selection



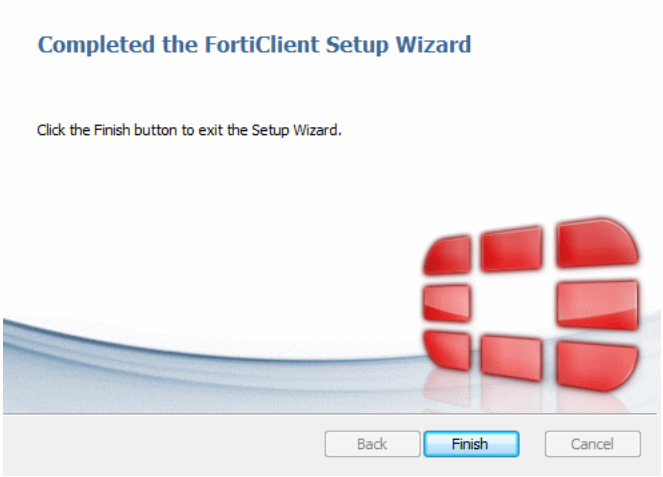
4. Select Install to continue.

Figure 4: Ready to install FortiClient


Ready to install FortiClient
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

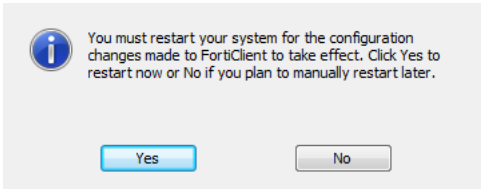
5. Select Finish to exit the FortiClient Setup Wizard.

Figure 5: Installation completed



6. On a new FortiClient installation, you do not need to reboot your system. When upgrading the FortiClient version, you must restart your system for the configuration changes made to FortiClient to take effect. Select *Yes* to restart your system now, or select *No* to manually restart later.

Figure 6: System Restart Confirmation


You must restart your system for the configuration changes made to FortiClient to take effect. Click Yes to restart now or No if you plan to manually restart later.
Yes
No

7. To launch FortiClient, double-click the desktop shortcut icon.

Figure 7: Select the FortiClient shortcut to launch

Installing FortiClient on a Mac OS X computer

The following instructions will guide you though the installation of FortiClient on a Mac OS X computer.

To install FortiClient

1. Double-click the FortiClient .dmg installer file to launch the FortiClient installer. The *FortiClient Installer* will install FortiClient on your computer. Select *Continue*.

Figure 8: Welcome screen

Install FortiClient
Welcome to the FortiClient Installer
Introduction
License
Destination Select
Installation Type
Installation
Summary
FortiClient for Mac OS X is a unified security agent for computers that integrates antivirus, SSL and IPSec VPN remote access, web filtering, firewall and vulnerability scan into a single software package. FortiClient for Mac OS X has a user-friendly interface that allows for quickly setting up protection for your computer.
Go Back
Continue

2. Read the Software License Agreement and select *Continue*. You have the option to print or save the Software Agreement on this screen. You will be prompted to *Agree* with the terms of the license agreement.

Figure 9: Software License Agreement

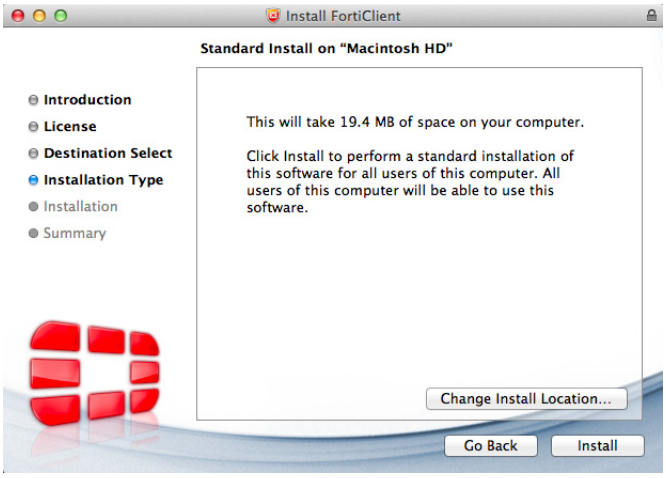
Install FortiClient
Software License Agreement
English
Introduction
License
Destination Select
Installation Type
Installation
Summary
Fortinet Product License Agreement / EULA and Warranty Terms
Trademarks and Copyright Statement
Fortinet®, FortiGate®, and FortiGuard® are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks, registered or otherwise, of Fortinet. All other product or company names may be trademarks of their respective owners. Copyright © 2002-2011 Fortinet, Inc., All Rights reserved. Contents and terms are subject to change by Fortinet without prior notice. No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet, Inc., as stipulated by the United States Copyright Act of 1976.
Product License Agreement
CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (THE OR THIS "AGREEMENT" OR "EULA"). USE OF FORTINET, INC. ("FORTINET") PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STANDALONE SOFTWARE PRODUCTS SOLD BY FORTINET
Print...
Save...
Go Back
Continue

3. Select the destination folder for the installation.

Figure 10: Destination Select screen

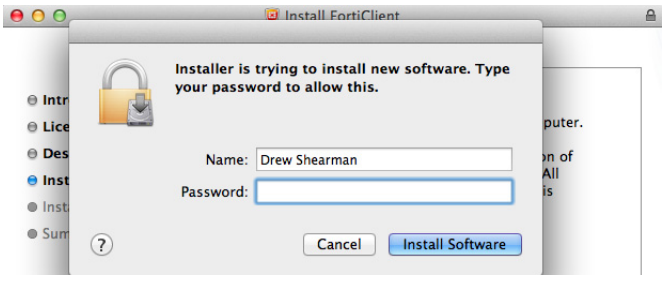
4. Select *Install* to perform a standard installation on this computer. You can change the install location from this screen.

Figure 11: Installation Type screen


Install FortiClient
Standard Install on "Macintosh HD"
Introduction
License
Destination Select
Installation Type
Installation
Summary
This will take 19.4 MB of space on your computer.
Click Install to perform a standard installation of this software for all users of this computer. All users of this computer will be able to use this software.
Change Install Location...
Go Back
Install

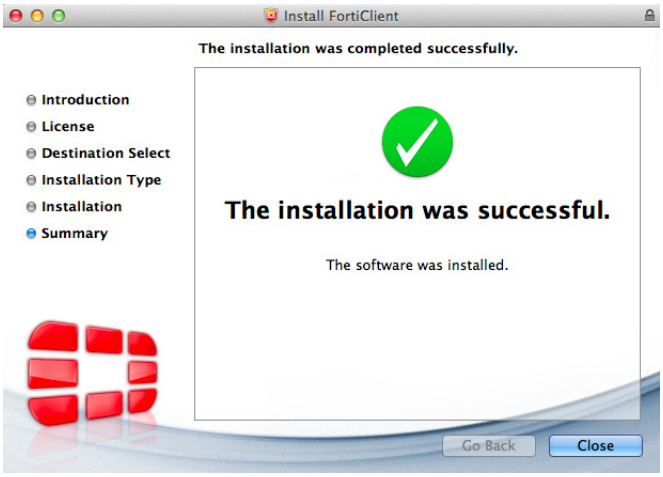
5. Depending on your system, you may be prompted to enter your system password.

Figure 12: Enter system password to continue


Installer is trying to install new software. Type your password to allow this.
Name: Drew Shearman
Password:
Cancel
Install Software

6. The installation was successful. Select *Close* to exit the installer.

Figure 13: The installation was successful

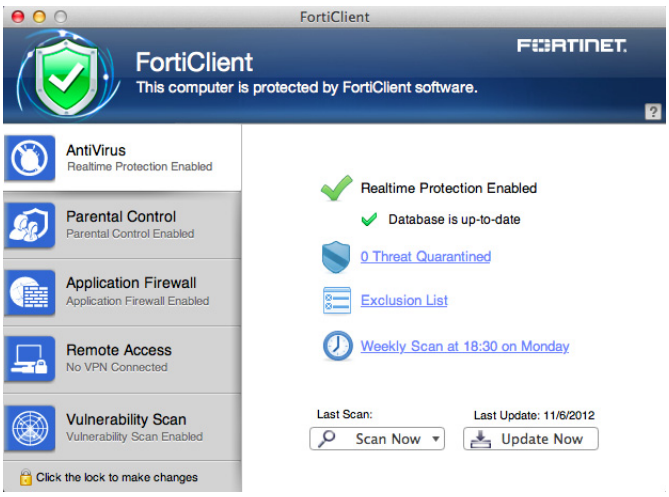


7. FortiClient has been saved to the Applications folder.

Figure 14: Applications folder

8. Double-click the FortiClient icon to launch the application. The application console loads to your desktop. Select the lock icon on the bottom left of the dashboard to make changes to the FortiClient configuration.

Figure 15: Default FortiClient dashboard is locked



Provisioning FortiClient

FortiClient MSI configuration tool

The FortiClient Configurator tool is the recommended method of creating a customized installation of FortiClient.

This document was written for FortiClient v5.0 Patch Release 1 for Windows. Not all features described in this document are supported for FortiClient v5.0 Patch Release 1 for Mac OS X.

Usage

```
FortiClientConfigurator.exe -m <path to FortiClient.msi file>
     [optional switches]
```

Switches and switch parameters are case sensitive.

```
-m <path to FortiClient msi file> (Required)
--REGISTRATIONKEY <key>
```

Use to prevent users from changing FortiClient settings.

```
--FGTIP <ip:port or fqdn:port>
```

FortiClient will attempt to register to this FortiGate. If it cannot, it will try to register to the default gateway.

Example usage

```
FortiClientConfigurator.exe -m c:\downloads\forticlient.msi
     --REGISTRATIONKEY sercretpassword
```

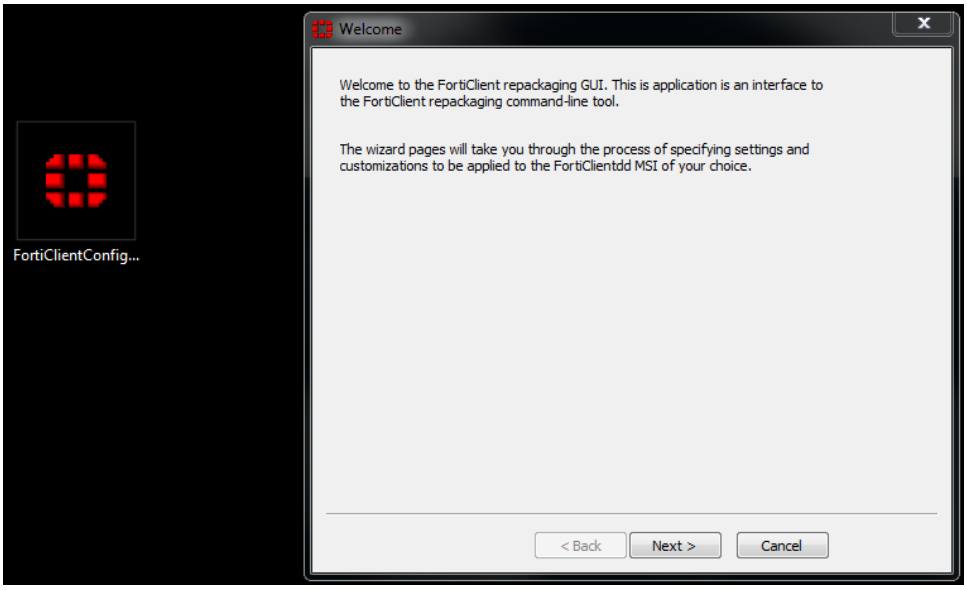
This command above creates the following directories containing files ready for deployment:

```
c:\downloads\FortiClient_packaged\ActiveDirectory\
c:\downloads\FortiClient_packaged\ManualDistribution\
```

FortiClient Configurator application

The FortiClientConfiguratorGUI tool is an application interface to the FortiClient repacking command line tool. The wizard will guide you through the process of specifying settings to be applied to the FortiClient MSI file.

Figure 16: FortiClient Configuration application interface


FortiClientConfig...
Welcome
Welcome to the FortiClient repackaging GUI. This is application is an interface to the FortiClient repackaging command-line tool.
The wizard pages will take you through the process of specifying settings and customizations to be applied to the FortiClientdd MSI of your choice.
< Back
Next >
Cancel

Creating a custom MSI installation file

You can create a custom MSI installer file for your customized FortiClient Application:

1. Determine the command line options you need for your customized FortiClient installer.
2. In the folder where you expanded the installer .zip package, execute the following command line entry:

   ```
   FortiClientConfigurator.exe -m <path to FortiClient.msi file>
        <optional switches>
   ```

   A new subdirectory is created, which contains the FortiClient MSI file.

For more information on FortiClient XML configuration, see the *FortiClient v5.0 XML Reference* at the Fortinet Technical documentation site, http://docs.fortinet.com.

Deploy FortiClient using Microsoft Active Directory (AD) server

There are multiple ways to deploy FortiClient to endpoint devices using Microsoft Active Directory.

The following instructions are based from Microsoft Windows Server 2008. If you are using a different version of Microsoft Server, your MMC or snap-in locations may be different.

Using Microsoft AD to Deploy FortiClient:

On your Domain Controller, create a distribution point.

1. Log on to the server computer as an administrator.

2. Create a shared network folder where the FortiClient MSI installer file will be distributed from.
3. Set file permissions on the share to allow access to the distribution package. Copy the FortiClient MSI installer package into this share folder.
4. Select *Start* > *Administrative Tools* > *Active Directory Users and Computers*.
5. After selecting your domain, right-click to select a new Organizational Unit (OU).
6. Move all the computers you wish to distribute the FortiClient software to into the newly-created OU.
7. Select *Start* > *Administrative Tools* > *Group Policy Managemen*t. The Group Policy Management MMC Snap-in will open. Select the OU you just created. Right-click it, *Select Create a GPO* in this domain, and Link it here. Give the new GPO a name then select OK.
8. Expand the Group Policy Object container and find the GPO you just created. Right-click the GPO and select Edit. The Group Policy Management Editor MMC Snap-in will open.
9. Expand *Computer Configuration* > *Policies* > *Software Settings*. Right-click Software Settings and select *New* > *Package*.
10. Select the path of your distribution point and FortiClient installer file and then select *Open*. Select *Assigned* and select *OK*. The package will then be generated.
11. If you wish to expedite the installation process, on both the server and client computers, force a GPO update.
12. The software will be installed on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and install the software then.

Uninstall FortiClient using Microsoft Active Directory server

This section describes how to remove FortiClient from client computers using Active Directory:

1. On your domain controller, select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in will open. Expand the Group Policy Objects container and right-click the Group Policy Object you created to install FortiClient and select Edit. The Group Policy Management Editor will open.
2. Select *Computer Configuration* > *Policy* > *Software Settings* > *Software Installation*. You will now be able to see the package that was used to install FortiClient.
3. Right-click the package, select *All Tasks* > *Remove*. Choose Immediately uninstall the software from users and computers, or *Allow* users to continue to use the software but prevent new installations. Select *OK*. The package will delete.
4. If you wish to expedite the uninstallation process, on both the server and client computers, force a GPO update as shown in the previous section. The software will be uninstalled on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and uninstall the software then.

Deploy using Microsoft System Center Configuration Manager 2007

If you would like to use Microsoft's System Center Configuration Manager (SCCM) to deploy FortiClient, use the following method:

These instructions assume you have already installed and configured SCCM. If you have not, please refer to Microsoft's online help sources for information on this task.

Step 1: Create Your Package

1. Startup your Configuration Manager Console GUI and expand the following: *Computer Management* > *Software Distribution* > *Packages*.
2. Right-click Packages and select *New* > *Package* from the contextual menu. A Wizard will open.
3. Fill in the packages properties as you desire in the General tab.
4. Under the Data Source tab, select the *This package contains source files* box, then select the Set button to specify the source of the SCCM package. SCCM will then ask you to specify the path to the installation executable. Select that path, then select OK.
5. Select the box adjacent to *Update distribution points on a schedule* and then set the schedule to how often you wish.
6. Set your *Data Access* options if required.
7. Under the Distribution Settings tab, set your sending priority. *High* is recommended.
8. Under the *Reporting* tab, leave the settings as default.
9. Under the *Security* tab, set the rights for the package class and instance rights.
10. Review your package choices under the *Summary* tab, then select *Next*. The Wizard will complete.

Step 2: Create a Program for Your Package

1. Startup your Configuration Manager Console GUI and expand the following:

   Computer Management > *Software Distribution* > *Packages*.

   Select the newly-created FortiClient package. Right-click that package and select *New* > *Program* from the contextual menu.
2. Under the General tab, fill in the appropriate details. For a silent install, ensure you use the `-ms switch` under the command line options.
3. Under the Requirements tab, check the boxes next to the client platforms you wish to install to (Windows Vista, Windows XP, etc.).
4. Set your Environment variables. It is recommended to select that the program can run *Whether or not a user is logged on*.
5. You can leave the *Advanced* and *Windows* Installer tabs as default.
6. If you require a notification sent to Microsoft Operations Manager (MOM), select the appropriate options under the MOM Maintenance tab.
7. As with the previous step, review your Summary and then create your program.

Step 3: Advertising Your Package to Client PCs

1. Startup your Configuration Manager Console GUI and expand the following:

   Computer Management > *Software Distribution* > *Advertisements*.

   Right-click Advertisements and select *New* > *Advertisement* from the contextual menu.
2. When prompted about no distribution points, select Yes. We will update the distribution point later in the process.
3. Under the Schedule tab, set the date you wish the advertisement to commence (and expire, if you desire). Set your priority level (recommended setting is “High”). Select on the yellow star to set the mandatory settings.
4. Under the Distribution Points tab, select “Download content from distribution point and run locally” for both settings.
5. Under the Interaction tab, you can use this to warn logged in users that the program is going to run and provide a countdown timer until execution.
6. Under the Security tab, set the rights for the package class and instance rights.

7. Review your package choices under the Summary tab, then select Next. The Wizard will complete.

Step 4: Create and Update Your Distribution Point

1. Startup your Configuration Manager Console GUI and expand the following:

   Computer Management > *Software Distribution* > *Packages*.

   Expand the package you created and right-click Distribution Points.

   Right-click *Distribution Points* and select *New Distribution Points* from the contextual menu. A Wizard will open.
2. Select your SCCM server from the list of available servers and select *Next*. You will then see a summary and the Wizard will complete.
3. You will now need to update the distribution point that was just created with the advertisement package. Right-click Distribution Points and now select Update Distribution Points from the contextual menu. A pop-up window will appear. Confirm the update by selecting *Yes*.

Using Microsoft SCCM 2007 to Remove FortiClient:

1. Open the Configuration Manager Console:

   System Center Configuration Manager > *Site Database* > *Computer Management* > *Software Distribution* > *Package* > *Advertisement*.
2. Select the FortiClient package you wish to uninstall, then select Per-system uninstall. Ensure you select the correct boundary collection. Specify when the advertisement will broadcast to the members of the target collection.
3. Complete the Wizard. Ensure you delete the initial Installation Advertisement you used to install FortiClient to prevent SCCM from reinstalling FortiClient.

Endpoint Management

Introduction

The purpose of this section is to provide basic instructions on how to configure, deploy, and manage FortiClient configurations from FortiGate.

Endpoint Management requires FortiClient v5.0.0 GA or later and a FortiGate (FortiGate, FortiWiFi, FortiGate-VM) running FortiOS v5.0.0 GA or later and FortiCarrier devices running FortiOS Carrier v5.0.0 GA or later.

Endpoint Management is available on the FortiGate 40C and higher devices.

Configure Endpoint Management

In FortiOS v5.0, configuration and management of FortiClient endpoint agents can now be handled by the FortiGate. You can configure your FortiGate device to discover new devices on your network, enforce FortiClient registration, and deploy a pre-configured endpoint profile to connected devices. The endpoint profile can be deployed to devices on your network and over a VPN connection.

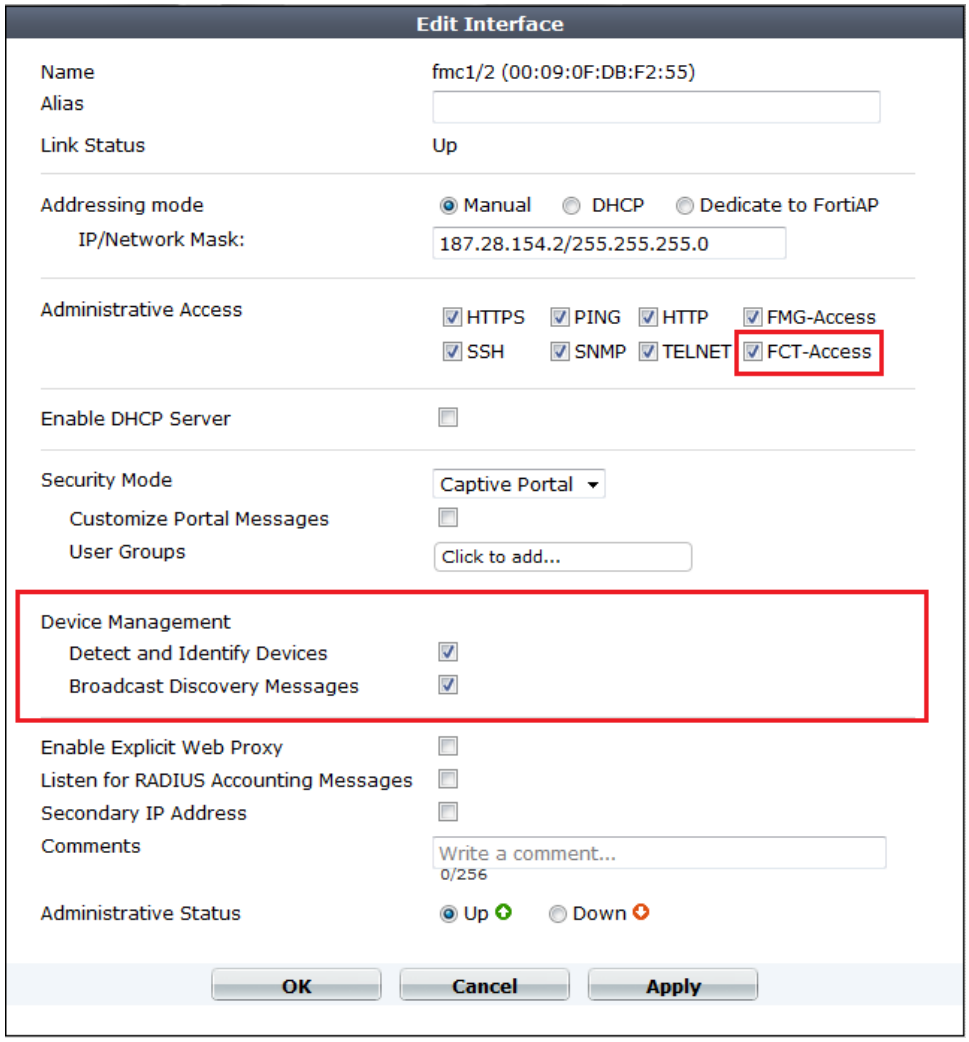
To configure Endpoint Management on the FortiGate, follow the steps listed below.

Step 1: Enable Device Management and Broadcast Discovery Messages

To configure *Device Management,* go to *System* > *Network* > *Interface,* select the interface, and select *Edit* on the toolbar. On the *Edit Interface* page you can select to enable *Detect and Identify Devices.* To enable *Broadcast Discovery Messages* (optional) you must first enable *FCT-Access* under *Administrative Access*. Select *Apply* to save the setting.

Broadcast Discovery Messages is an optional configuration. When enabled, the FortiGate will broadcast messages to your network, allowing client connections to discover the FortiGate for FortiClient registration. Without this feature enabled, the user will enter the IP address or URL of the FortiGate to complete registration.

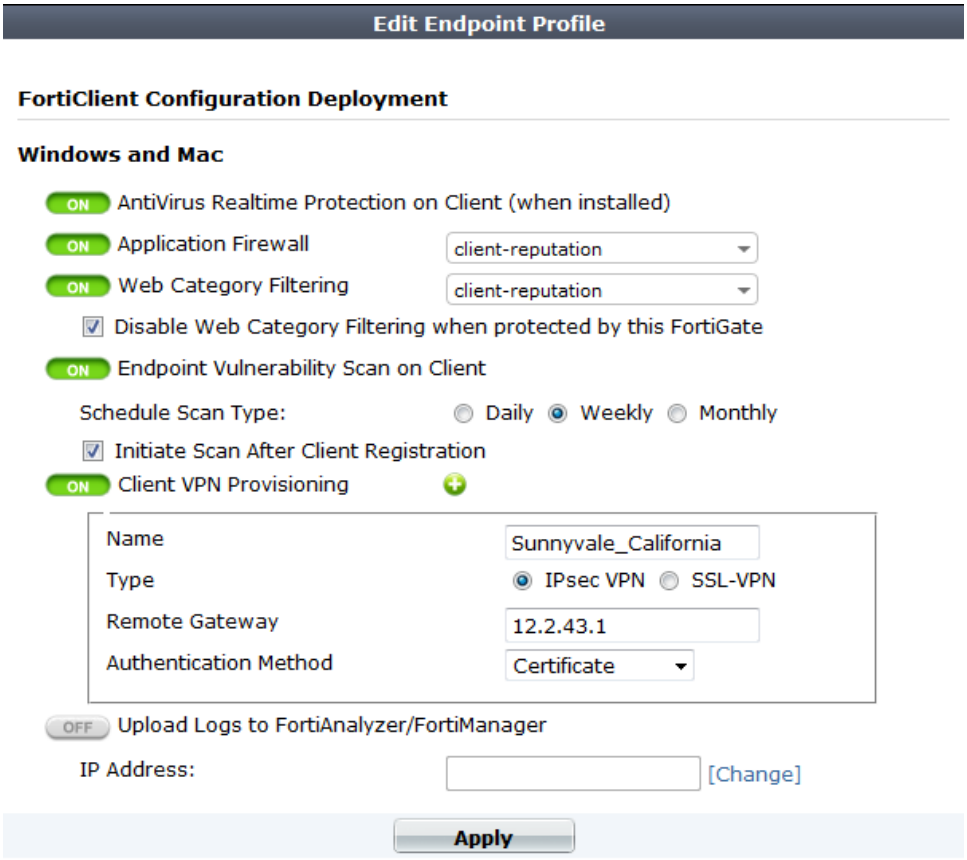
Figure 17: Device Management options



Step 2: Configure the Client Endpoint Profile

To configure the *Client Endpoint Profile*, go to *User & Device* > *Device* > *Endpoint Profile*. Edit as required. Select *Apply* to save the setting.

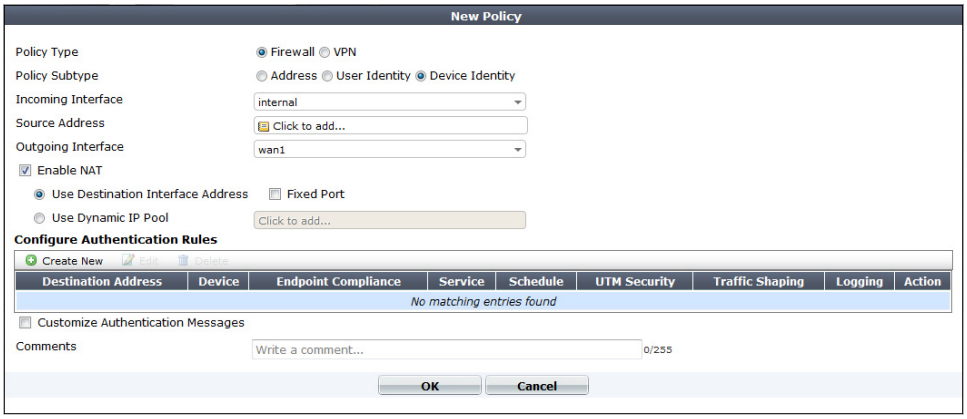
Figure 18: Edit endpoint profile



Step 3: Configure Firewall Policies

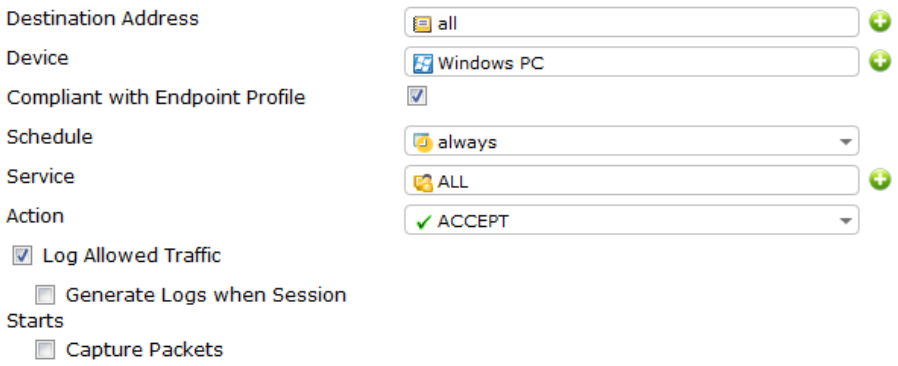
To configure a firewall policy for Endpoint Management, go to *Policy* > *Policy* > *Policy* and select *Create New* on the right-hand toolbar. For *Policy Subtype*, select *Device Identity*.

Figure 19: Create new device identity policy



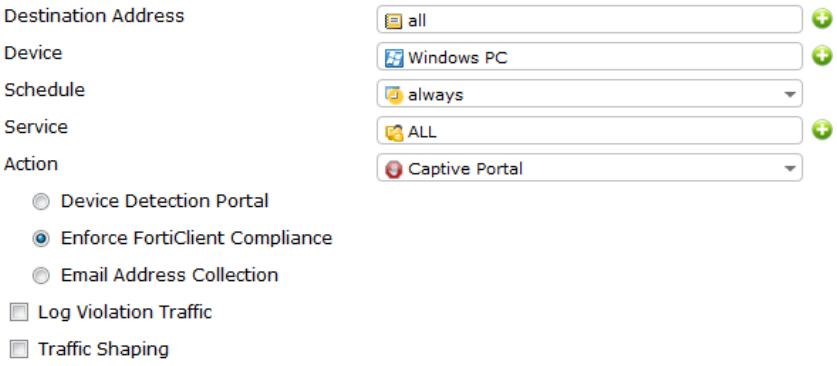
Add an *Accept* authentication rule for all compliant Windows-PC clients. This rule will allow Windows clients which have installed FortiClient and have been registered to this FortiGate to pass traffic.

Figure 20: Accept authentication rule for compliant Windows-PC clients.



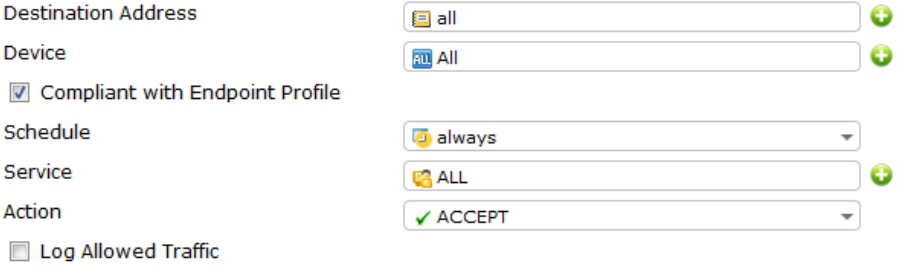
Add a *Captive Portal a*uthentication rule for all non-compliant Windows-PC clients. This rule will redirect all Windows clients (via a web browser) to a dedicated portal where they can download the client. Once registered to the FortiGate, the Endpoint Profile will be assigned.

Figure 21: Captive portal authentication rule for Windows-PC devices.



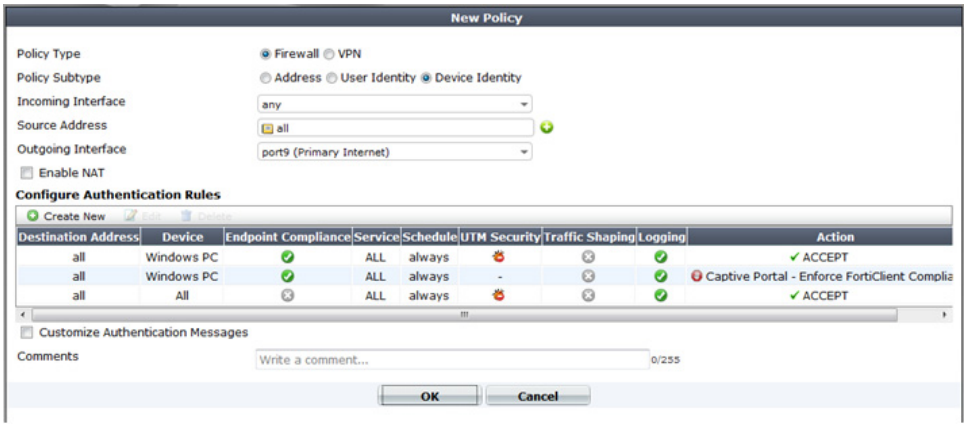
(Optional) Add an *Accept a*uthentication rule to allow traffic from all other devices to pass traffic without enforcing FortiClient Compliance.

Figure 22: Accept Authentication Rule for all other devices



Once these three authentication rules are configured, select *OK* to save the new policy setting. Your client configuration is ready for deployment.

Figure 23: Firewall policy configuration



After the FortiGate configuration has been completed, you can proceed with FortiClient configuration. Configure your Windows PC on the corporate network with the default gateway set to the IP of the FortiGate.

FortiClient Endpoint network topologies

The following FortiClient Endpoint Profile topologies are supported:

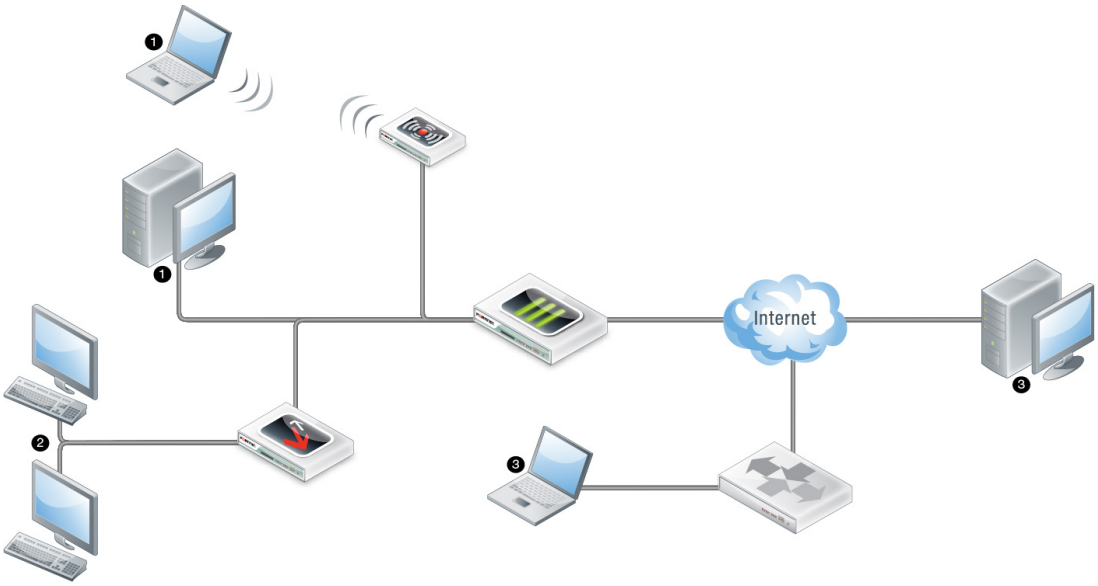
- Client is directly connected to FortiGate; either to a physical port, switch port or WiFi SSID.[1]

  This topology supports client registration, configuration sync, and endpoint profile enforcement.
- Client is connected to FortiGate, but is behind a router or NAT device.[2]

  This topology supports client registration and configuration sync.
- Client is connected to FortiGate across a VPN connection.[3]

  This topology supports client registration, configuration sync, and endpoint profile enforcement.

Figure 24: Network topologies

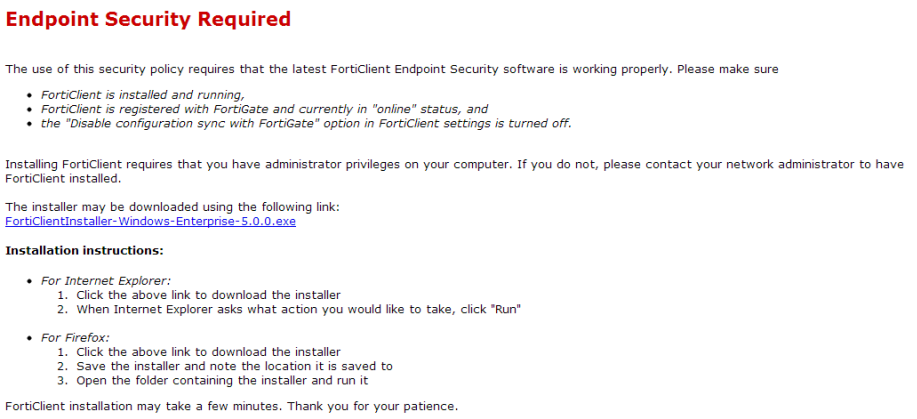


To configure FortiClient for Endpoint Management, follow the steps listed below.

Step 1: Download and install FortiClient

Open a web browser from your workstation and attempt to open a web page, the web page will be directed to the Captive Portal. Follow the instructions on the portal to download and install FortiClient.

Figure 25: Captive Portal block page is displayed.



Endpoint Security Required

The use of this security policy requires that the latest FortiClient Endpoint Security software is working properly. Please make sure

- *FortiClient is installed and running,*
- *FortiClient is registered with FortiGate and currently in "online" status, and*
- *the "Disable configuration sync with FortiGate" option in FortiClient settings is turned off.*

Installing FortiClient requires that you have administrator privileges on your computer. If you do not, please contact your network administrator to have FortiClient installed.

The installer may be downloaded using the following link:
FortiClientInstaller-Windows-Enterprise-5.0.0.exe

Installation instructions:

- *For Internet Explorer:*
  1. Click the above link to download the installer
  2. When Internet Explorer asks what action you would like to take, click "Run"
- *For Firefox:*
  1. Click the above link to download the installer
  2. Save the installer and note the location it is saved to
  3. Open the folder containing the installer and run it

FortiClient installation may take a few minutes. Thank you for your patience.

Step 2: FortiClient registration

After FortiClient completes installation, FortiClient will automatically launch and search for a FortiGate device for registration. There are three ways that the FortiClient/FortiGate communication is initiated:

1. FortiClient connects to the preferred IP address (if provided).
2. If 1. fails, FortiClient will attempt to connect to the default gateway IP address.
3. If 2. fails, FortiClient will listen for FortiGate broadcast messages.

Your personal computer's default gateway IP should be configured to be the IP set on the FortiGate interface.

Figure 26 shows an example broadcast message sent by the FortiGate and received by FortiClient. Select *Accept* to register with this FortiGate device. Upon registration, the FortiGate will send the Endpoint Profile to FortiClient.

Figure 26: FortiGate broadcast message

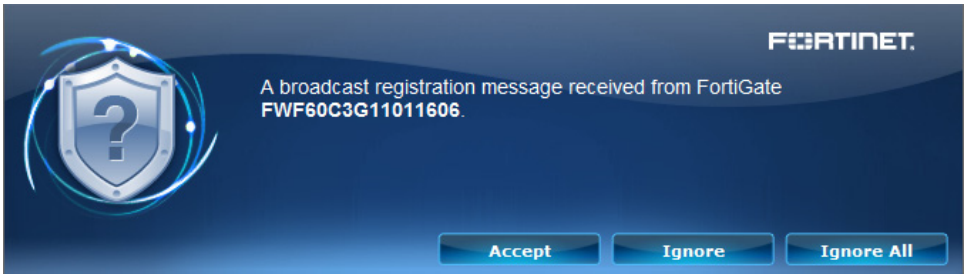


Figure 27 shows the behavior of FortiClient on initial setup. FortiClient will search for available FortiGate devices to complete registration. Select the *FortiGate* icon on the FortiClient dashboard to retry the search.

Figure 27: FortiClient will search for an available FortiGate

If FortiClient is unable to detect a FortiGate device, enter the IP address or URL of the device and select the *Retry* button as illustrated in Figure 28.

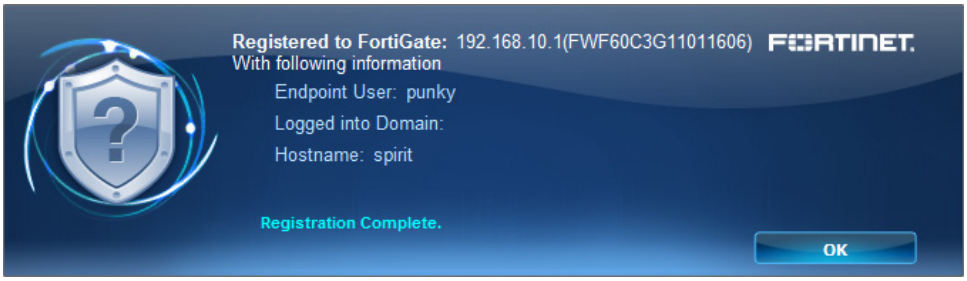
Figure 28: Enter the FortiGate IP or URL

When FortiClient locates the FortiGate, you will be prompted to confirm the registration as illustrated in Figure 29. Select the *Confirm* button to complete registration.

Figure 29: Registration confirmation window

Upon successful registration, the FortiGate will deploy the endpoint configuration.

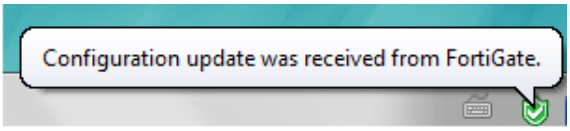
Figure 30: Registration complete



Step 3: FortiGate deploys the Endpoint Profile

The FortiGate will deploy the Endpoint Profile after registration is complete. This Endpoint Profile will permit traffic through the FortiGate. A system tray bubble message will be displayed once update is complete.

Figure 31: Configuration update notification message



The FortiClient console will display that it is successfully registered to the FortiGate. The Endpoint Profile is installed on FortiClient.

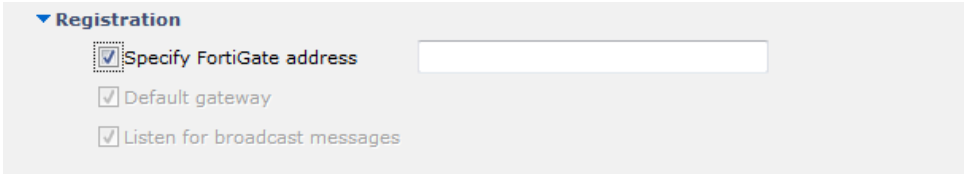
Figure 32: Registered FortiClient console

Deploy the Endpoint Profile to clients over VPN

You can deploy the Endpoint Profile to clients over a VPN connection.

1. On the FortiGate dashboard, select *File* > *Settings*. Under *Registration* select *Specify FortiGate address* and enter the IP address and port number (if required) of the FortiGate's internal interface.

Figure 33: Preferred FortiGate address

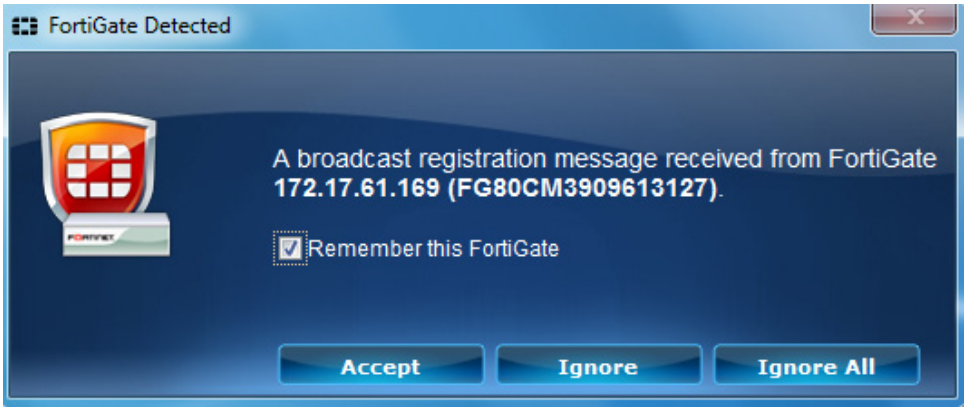


2. Configure an IPsec VPN connection from FortiClient to the management FortiGate. For more information on configuring IPsec VPN see "Create a new IPsec VPN connection" on page 50.
3. Connect to the VPN.
4. You can now search for the FortiGate gateway. See "Step 2: FortiClient registration" on page 28 for more information.
5. After registration, the client is able to receive the Endpoint Profile.

Remembered FortiGates

FortiClient v5.0 Patch Release 1 adds the option to remember the FortiGate when accepting the broadcast registration message.

Figure 34: Option to remember FortiGate



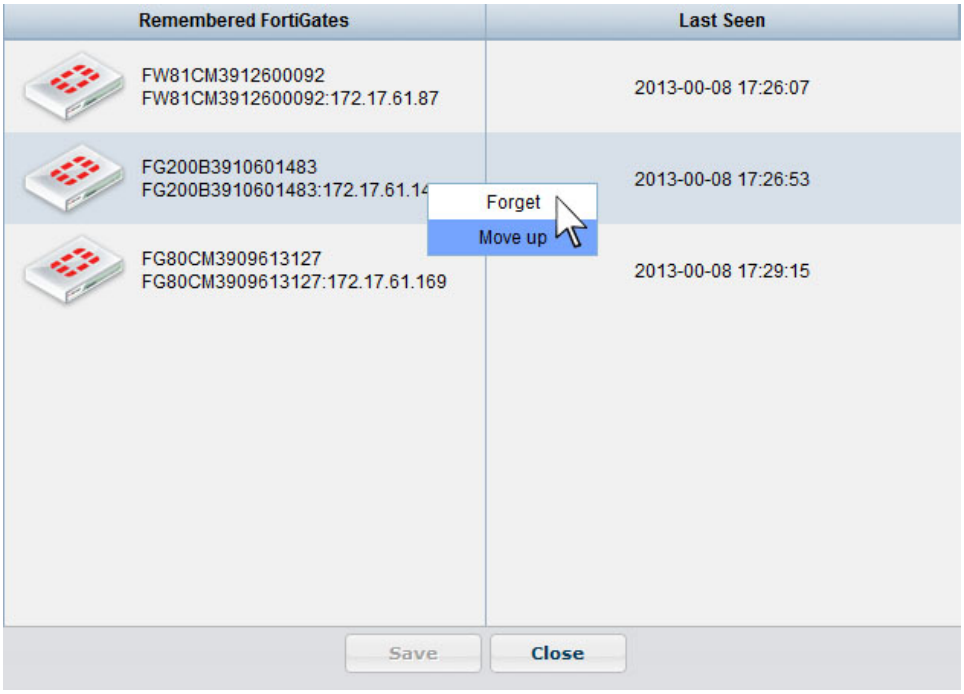
This feature will be enhanced in future patch releases to allow FortiClient to automatically switch between different remembered devices.

Select the registration icon on the dashboard to view information for the current registered device including the hostname, domain, serial number, and IP address.

Figure 35: Remembered FortiGates

Select *Remembered FortiGates* to show a list of FortiGate devices that FortiClient has previously registered with. Use the right-click menu to forget a specific device. Select the device that you would like to remove from the remembered FortiGates list, right-click, and select *Forget.* You can also change the order of devices in this list using the right-click menu.

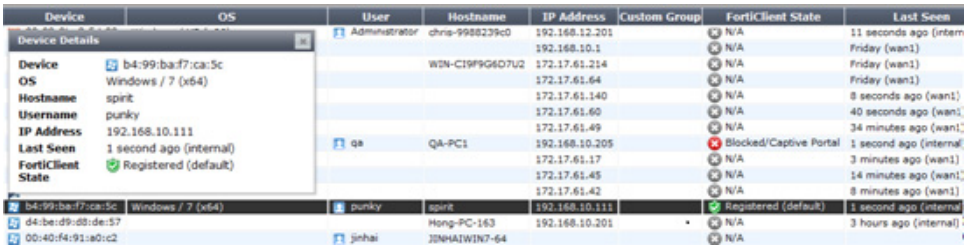
Figure 36: Show remembered devices



View FortiClient registration on the FortiGate Web-based Manager

You can view all registered FortiClient on the FortiGate Web-based Manager. Each new registration will be automatically added to the device table. To view registered devices go to *User & Devices* > *Device* > *Device Definition*. The state for the new FortiClient registration is listed as *Registered*.

Figure 37: FortiGate device

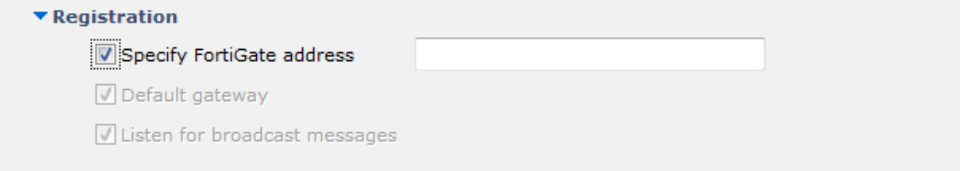


Configure preferred FortiGate IP on FortiClient for registration

The FortiClient admin user can specify a preferred FortiGate IP address for registration and client configuration management. When an unregistered FortiClient starts up, it first looks for the preferred FortiGate. If the preferred FortiGate is not reachable, it will look to connect to default gateway. If both the preferred FortiGate and default gateway are not reachable, FortiClient will listen for the broadcast message from FortiGate.

To configure a preferred FortiGate IP address on FortiClient, go to *File* > *Settings.* Select Registration to expand the drop-down menu. Enter the IP address and port number (if required) of the FortiGate's internal interface.

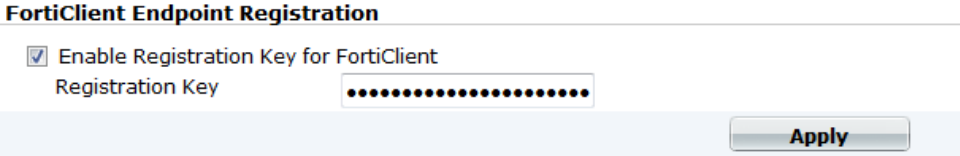
Figure 38: Configure preferred FortiGate on FortiClient



Enable FortiClient Endpoint Registration (optional)

To enable FortiClient Endpoint Registration on FortiClient, go to *System* > *Config* > *Advanced*. Select *Enable Registration Key for FortiClient*, enter the *Registration Key* and select *Apply*.

Figure 39: Enable FortiClient Endpoint Registration on FortiGate



The FortiClient user will need to enter the same registration key to successfully register FortiClient to the FortiGate.

Antivirus

FortiClient Antivirus

FortiClient v5.0 includes an Antivirus module to scan system files, executables, dll's, and drivers. FortiClient will also scan for and remove rootkits.

This section describes how to enable Antivirus and configuration options.

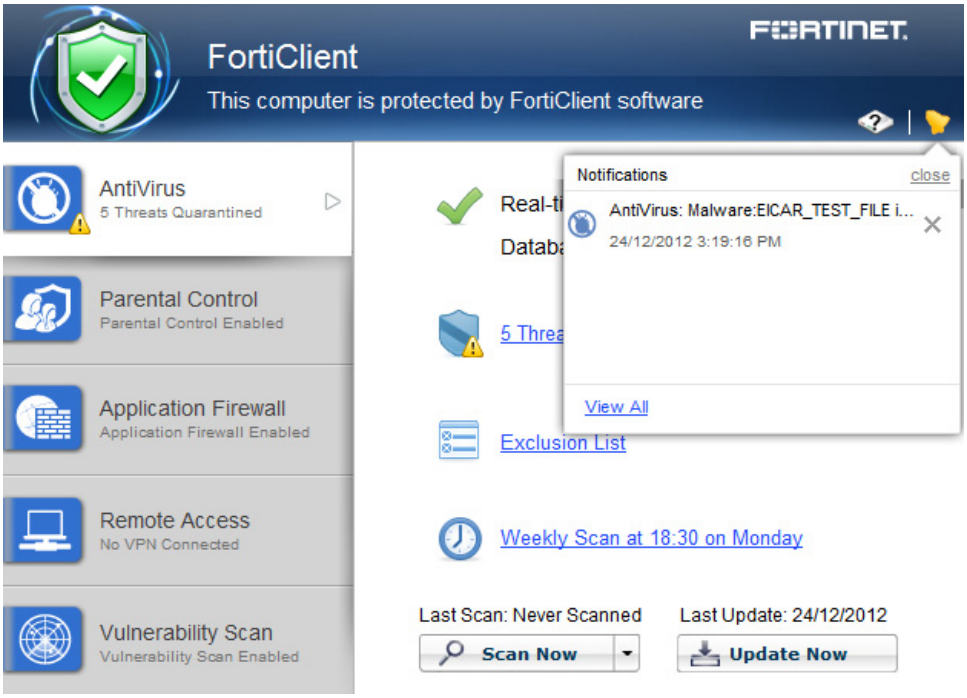
Enable/Disable Antivirus

To enable or disable FortiClient Real-time Protection, toggle the *[Enable/Disable]* option on the FortiClient dashboard.

Notifications

Select the bell icon on the FortiClient dashboard to view all notifications. When a virus has been detected, an exclamation icon will appear on the Antivirus tree-menu tab. The bell icon will change from gray to yellow. Select *View All* to view all Antivirus event notifications.

Figure 40: Notifications window



Scan Now

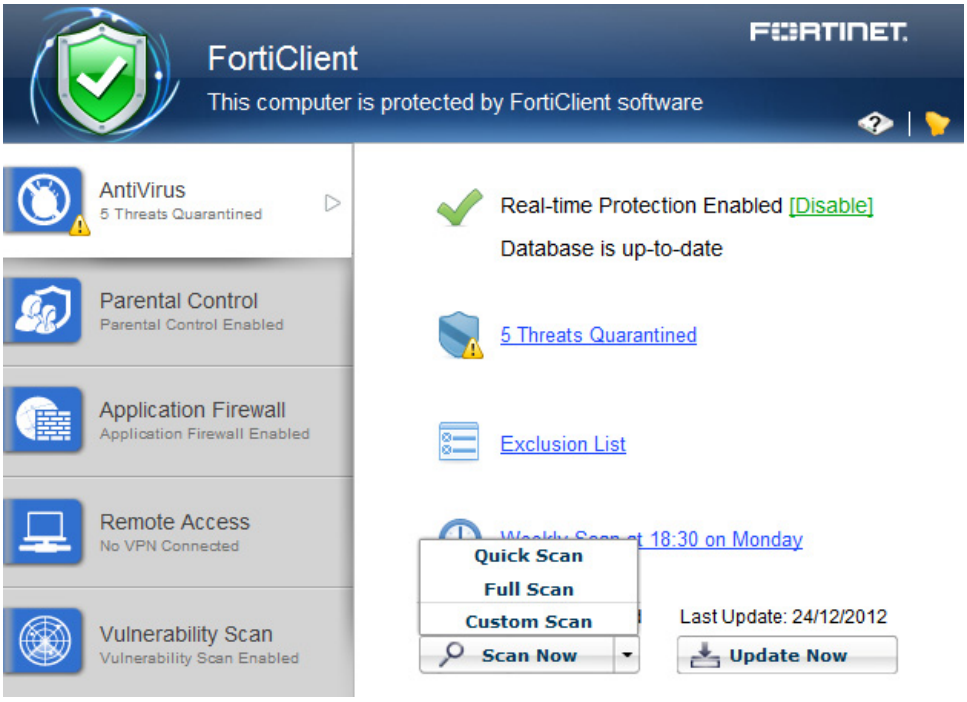
To perform on-demand antivirus scanning, select the *Scan Now* button on the FortiClient dashboard. Use the drop-menu to select *Custom Scan, Full Scan*, or *Quick Scan*. The dashboard notes the date of the last scan above the button.

Custom Scan runs the rootkit detection engine to detect and remove rootkits. *Custom Scan* allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats.

Full Scan runs the rootkit detection engine to detect and remove rootkits. *Full Scan* then performs a full system scan including all files, executables, dll's, and drivers for threats.

Quick System Scan runs the rootkit detection engine to detect and remove rootkits. *Quick System Scan* only scans executable files, dll's, drivers that are currently running for threats.

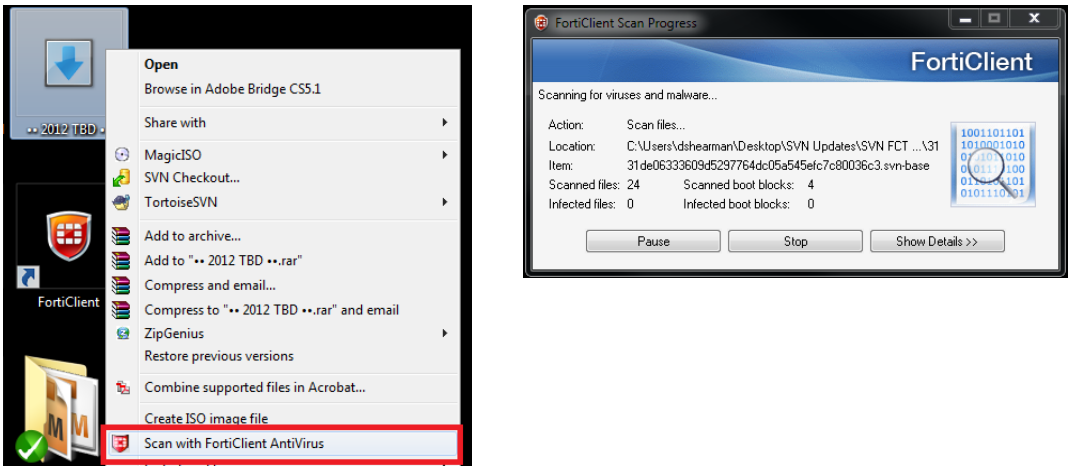
Figure 41: Antivirus scan options



Scan a file or folder

To perform a virus scan a specific file or folder, right-click the file or folder and select *Scan with FortiClient AntiVirus*.

Figure 42: Scan a specific file or folder

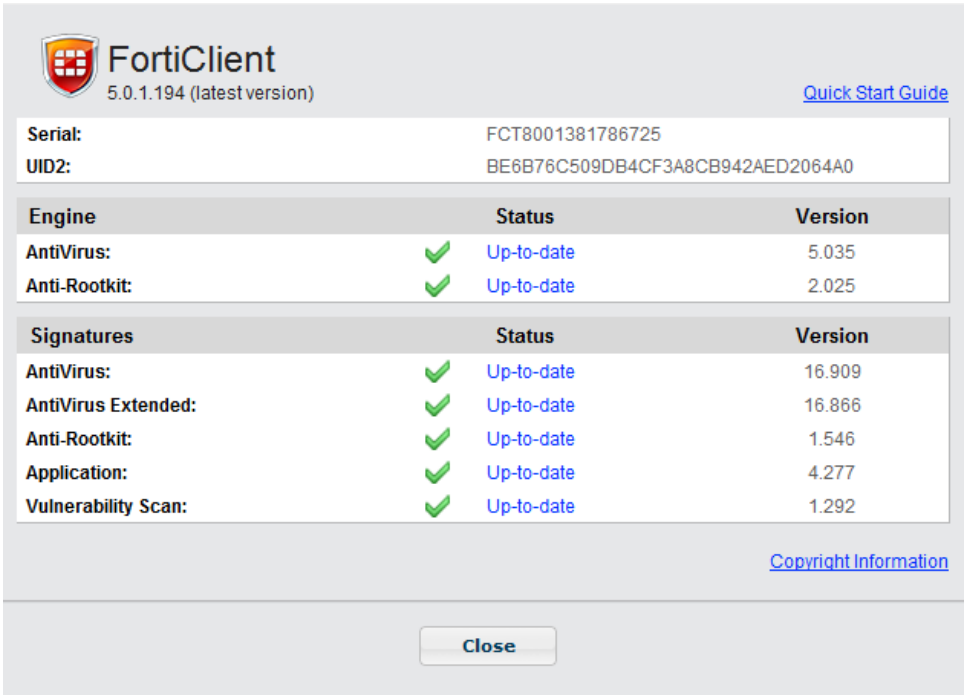


Update Now

To perform on-demand update of FortiClient version, engines, and signatures, select the *Update Now* button on the content pane. The content pane notes the date of the last update above the button.

To view the current FortiClient version, engine, and signature information, select *Help* on the toolbar, and *About* on the drop-down menu.

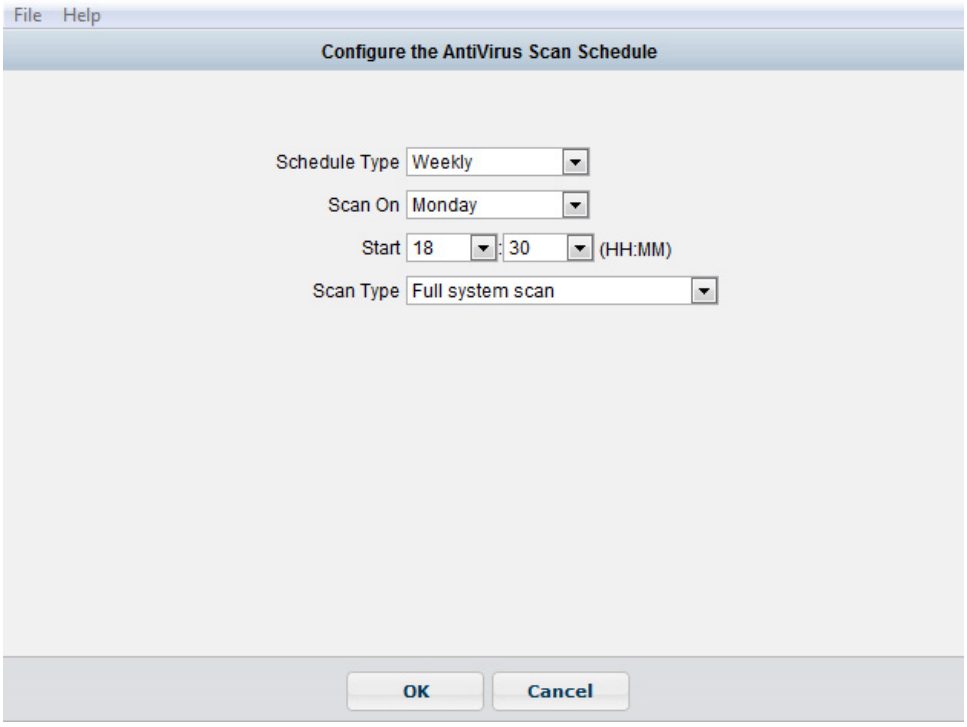
Figure 43: About FortiClient page



Schedule Antivirus scanning

To schedule antivirus scanning, select *Weekly Scan* on the content pane. On this menu you can configure options outlined in the following figure and table.

Figure 44: Antivirus scheduling

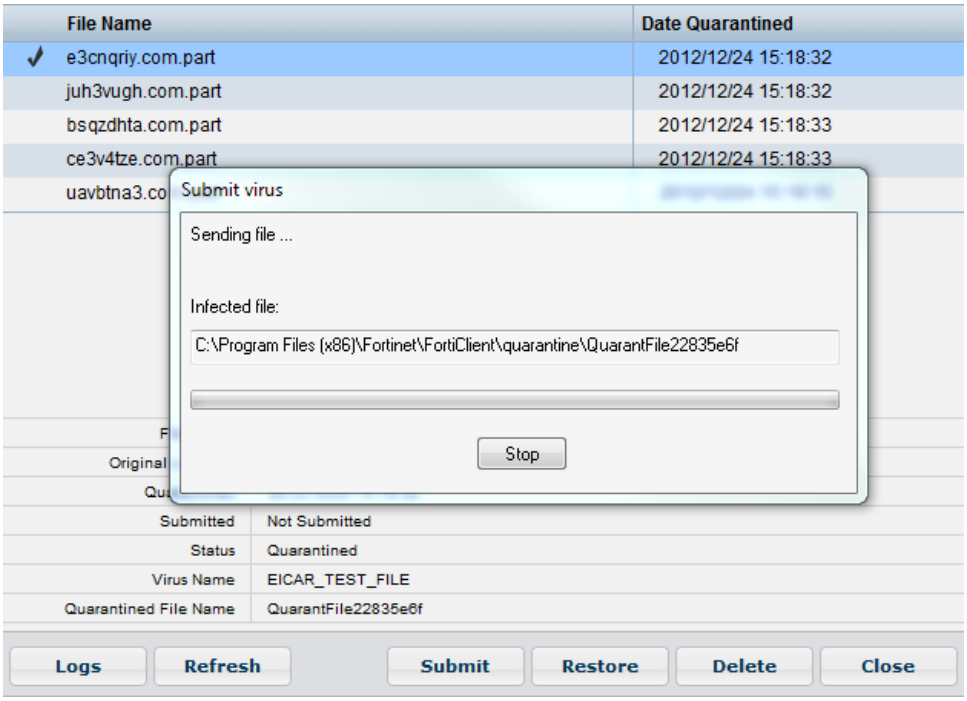


Schedule Type	Select Daily, Weekly or Monthly on the drop-down menu.
Scan On	For Weekly scheduled scan, select the day of the week on the drop-down menu. For Monthly scheduled scan, the day of the month on the drop-down menu.
Start	Select the start time on the drop-down menus. The time format is represented in hours and minutes, 24-hour clock.
Scan Type	Select the scan type: *Custom Scan* runs the rootkit detection engine to detect and remove rootkits. *Custom Scan* allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats. *Full Scan* runs the rootkit detection engine to detect and remove rootkits. *Full Scan* then performs a full system scan including all files, executables, dll's, and drivers for threats. *Quick System Scan* runs the rootkit detection engine to detect and remove rootkits. *Quick System Scan* only scans executable files, dll's, drivers that are currently running for threats.

View quarantined threats

To view quarantined threats, select *Threats Quarantined* on the FortiClient dashboard. On this page you can view, restore, or delete the quarantined file. You can also submit the file to FortiGuard.

Figure 45: Threats quarantined page

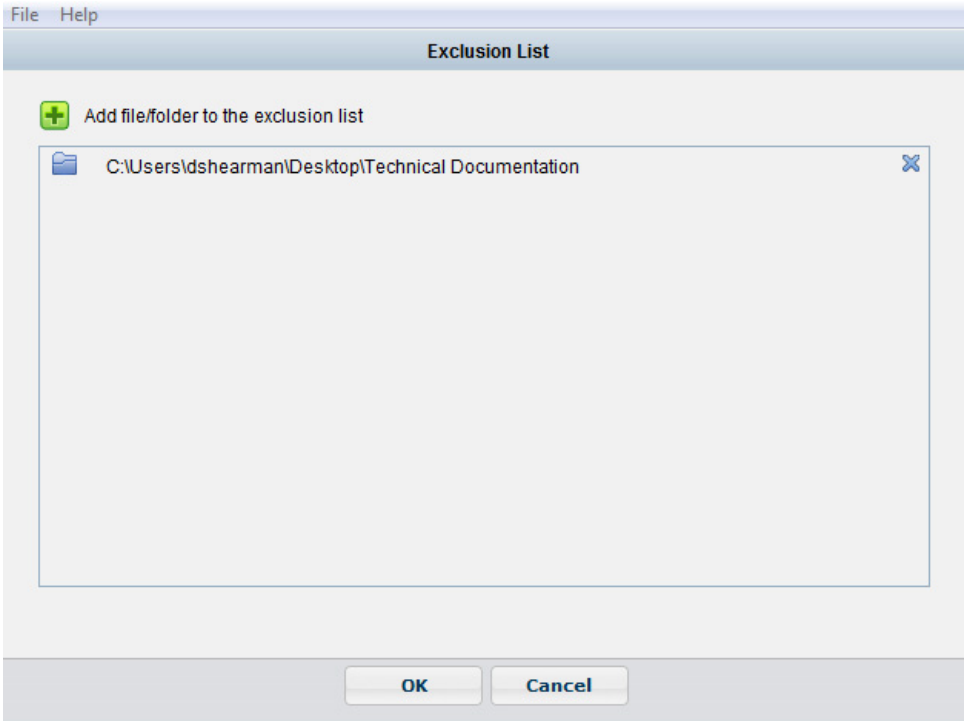


File Name	The name of the file.
Date Quarantined	The date and time that the file was quarantined by FortiClient.
File Information	Select a file from the list to view detailed information including the quarantined location, status, virus name, and quarantined file name.
Logs	Select to view FortiClient log data.
Refresh	Select to refresh the list.
Submit	Select to submit the quarantined file to FortiGuard.
Restore	Select to add the selected file/folder to the exclusion list.
Delete	Select to delete the quarantined file.
Close	Select to close the page and return to the FortiClient dashboard.

Add files/folders to an exclusion list

To add files/folders to the antivirus exclusion list, select *Exclusion List* on the content pane. On the following configuration page, select the '+' symbol to add files or folders to the list. Any files or folders on this exclusion list will not be scanned.

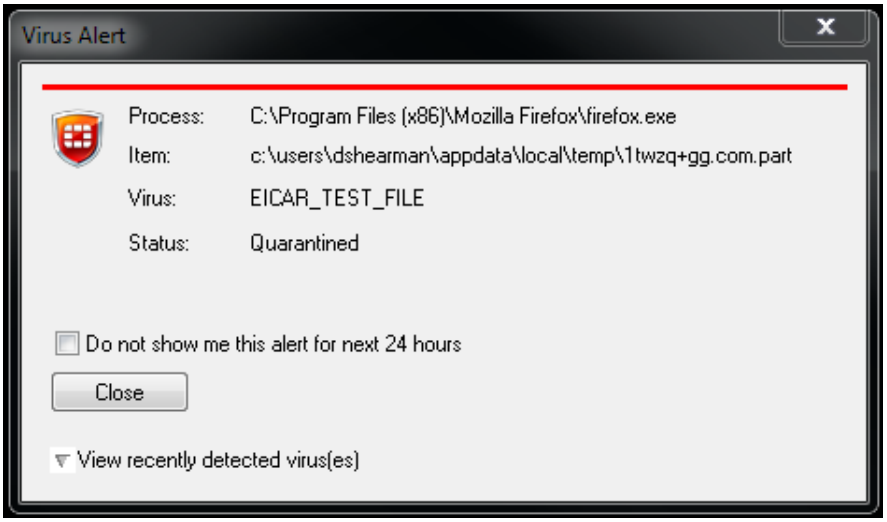
Figure 46: Antivirus Exclusion List



Antivirus warning

When FortiClient antivirus detects a virus while attempting to download a file via a web-browser, you will receive a warning dialog message similar to Figure 47. Browse to the *Threat Quarantine* menu on the dashboard to view details on the detected threat.

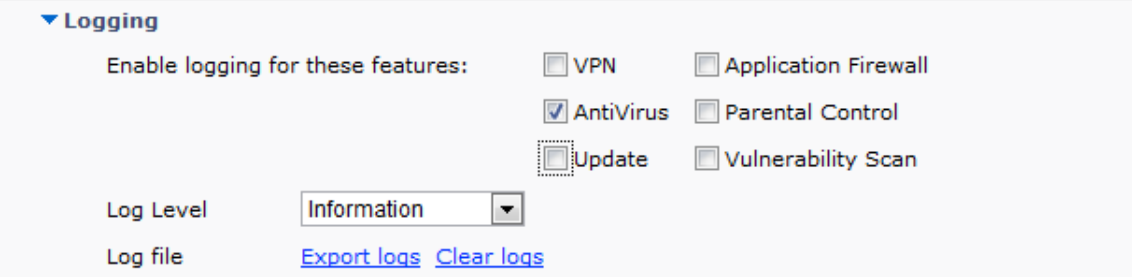
Figure 47: Example virus warning message



Antivirus logging

To configure antivirus logging, select *File* on the toolbar and *Settings* on the drop-down menu. Select *Logging* to view the drop-down menu. On this menu you can configure options outlined in the following figure and table.

Figure 48: Logging options

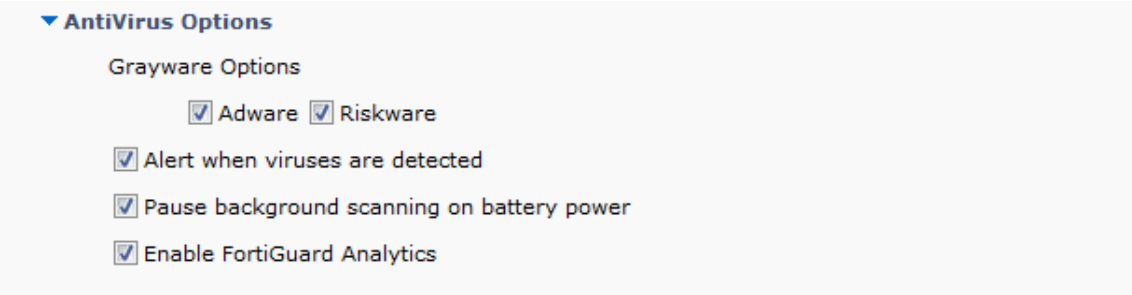


Logging	
Enable logging for these features	Select antivirus to enable logging for this feature.
Log Level	Select the level of logging: **Emergency:** The system becomes unstable. **Alert:** Immediate action is required. **Critical:** Functionality is affected. **Error:** An error condition exists and functionality could be affected. **Warning:** Functionality could be affected. **Notice:** Information about normal events. **Information:** General information about system operations. **Debug:** Debug FortiClient.
Log file	
Export logs	Select to export logs to your local hard disk drive (HDD) in .log format.
Clear logs	Select to clear all logs. You will be presented a confirmation window, select *Yes* to proceed.

Antivirus options

To configure antivirus options, select *File* on the toolbar, and *Settings* on the drop-down menu. Select *AntiVirus Options* to view the drop-down menu. On this menu you can configure options outlined in the following figure and table.

Figure 49: Antivirus options



Antivirus Options	
Grayware Options	Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge.
Adware	Select to enable adware detection and quarantine during the antivirus scan.
Riskware	Select to enable riskware detection and quarantine during the antivirus scan.
Alert when viruses are detected	Select to have FortiClient provide a notification alert when a threat is detected on your personal computer.
Pause background scanning on battery power	Select to pause background scanning when your personal computer is operating on battery power.
Enable FortiGuard Analytics	Select to automatically send suspicious files to the FortiGuard Network for analysis.

Parental Control/Web Filtering

FortiClient Parental Control/Web Filtering

Parental Control/Web Filtering allows you to block, allow, warn, and monitor web traffic based on URL category. URL categorization is handled by the FortiGuard Network.

When FortiClient is registered to a FortiGate, the Parental Control module will reflect Web Filtering. You can disable Web Filtering on the FortiClient from the FortiGate. If the FortiClient device is behind a FortiGate, the client device will use the Web Filter profile on the FortiGate.

Enable/Disable Parental Control/Web Filtering

To enable or disable FortiClient Parental Control/Web Filtering, toggle the *[Enable/Disable]* button on the FortiClient dashboard. Parental Control is enabled by default.

Figure 50: Parental Control module

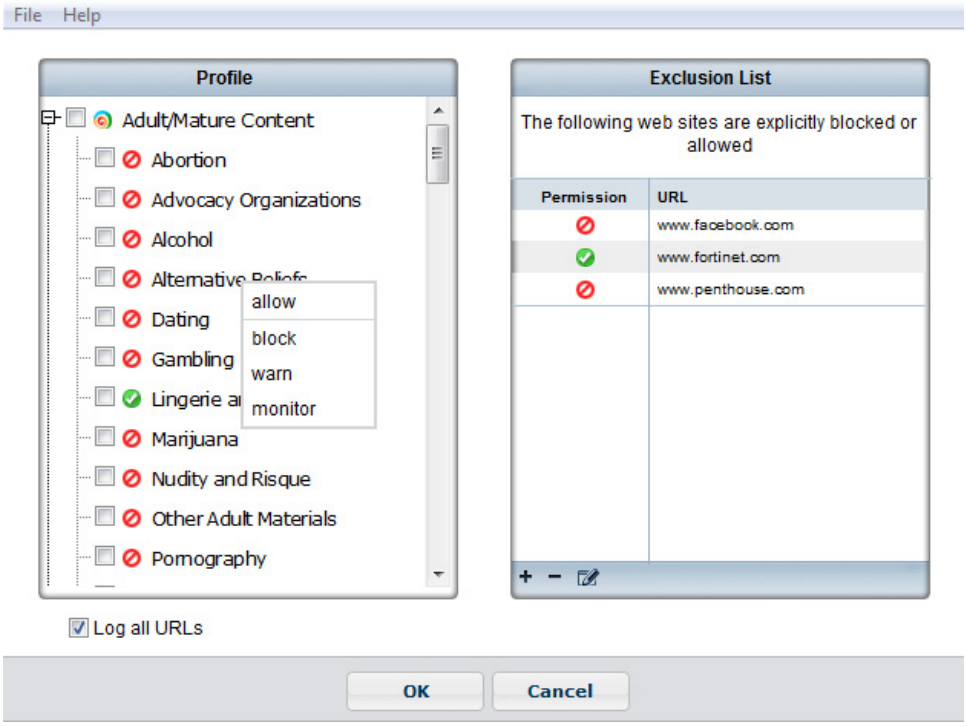
Enable/Disable	Toggle to enable or disable Parental Control.
Settings	Select to configure Parental Control profile.

Parental Control/Web Filtering settings

You can configure a profile to allow, block, warn, or monitor web traffic based on category under *Profile*. Use the right-click menu to set the action for the full category or sub-category.

You can add websites to the exclusion list and set the permission to allow or block. If the website is part of a blocked category, an allow permission on the *Exclusion List* would allow the user to access the specific URL.

Figure 51: Profile and exclusion list



View profile violations

To view profile violations, select *Violations (in the Last 7 Days)* on the FortiClient dashboard.

Figure 52: Traffic violations

Website	Category	Time	User
ffupdate.conduit-services.com	Malicious Websites	25/10/2012 9:53:37 AM	dshearman

Application Firewall

FortiClient Application Firewall

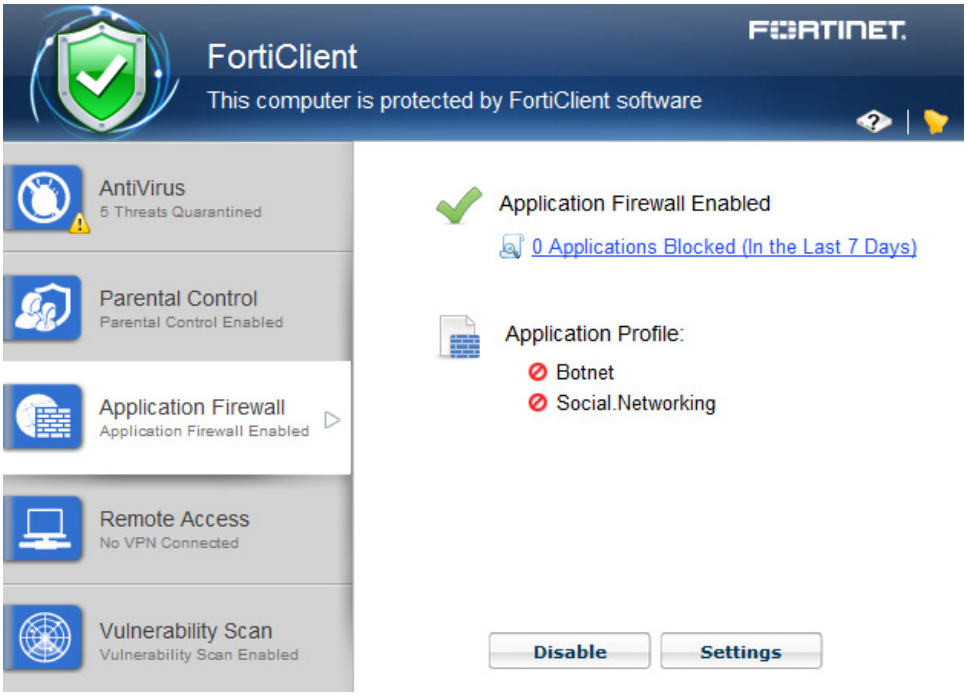
FortiClient v5.0 can recognize the traffic generated by a large number of applications. You can create rules to block or allow this traffic per category, or application.

This section describes how to enable the application firewall settings.

Enable/Disable Application Firewall

To enable or disable FortiClient Real-time Protection, select the *[Enable/Disable]* button on the FortiClient dashboard.

Figure 53: Application Firewall module



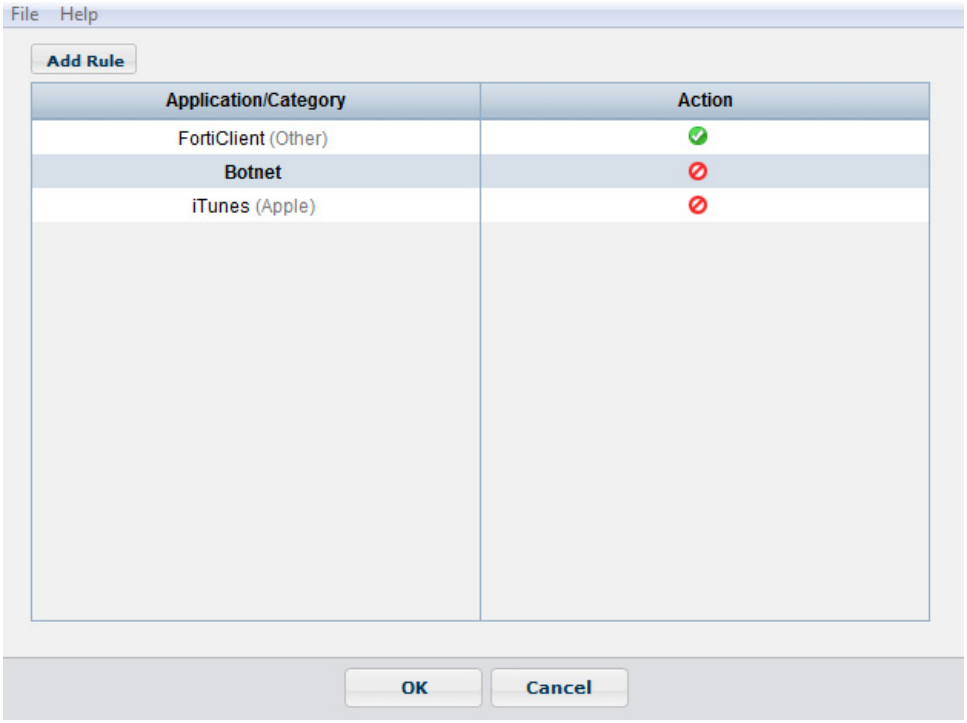
View Applications blocked

To view blocked applications, select *Applications Blocked* on the FortiClient dashboard This page lists all applications blocked in the past seven days, including the count and time of last occurrence.

Application Firewall rules

To view Application Firewall rules, select the *Settings* button on the FortiClient dashboard.

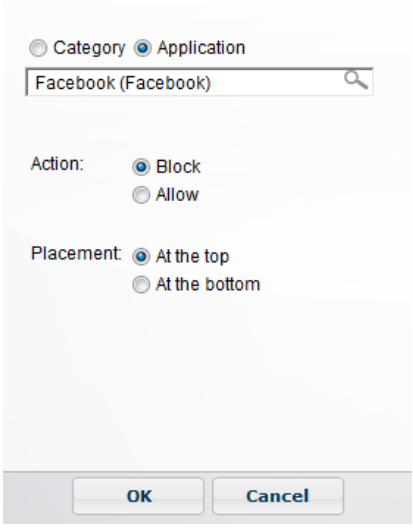
Figure 54: Application Firewall rules



To add a new rule

1. Select the *Add Rule* button.

Figure 55: Add rule window



2. Select either *Category* or *Application*. For category, use the drop-down list to select a category. For application, type either the full name of the application or first letter to search all applications starting with the selected letter.

FortiClient Application Firewall can only block applications for which FortiGuard has an application signature. You can submit a request to add a application signature on the FortiGuard site.

3. Select the action to *Block* or *Allow* the category or application.
4. Select placement of the rule *At the top* or *At the bottom*.
5. Select *OK* to save the setting.

To edit a rule

1. On the settings page, when you hover the mouse cursor on a rule, a hidden icon menu is available.
2. Select the edit icon to change the action of the rule.
3. Select the delete icon to remove the rule.
4. Select the move icon and drag-and-drop the rule to a new position on the list.
5. Select *OK* to save the setting and return to the FortiClient dashboard.

Application Firewall logging

To configure Application Firewall logging, select *File* on the toolbar, and *Settings* on the drop-down menu. Select *Logging* to view the drop-down menu. Select *Application Firewall* the logging menu to enable logging for this module.

IPsec VPN and SSL-VPN

FortiClient Remote Access (VPN)

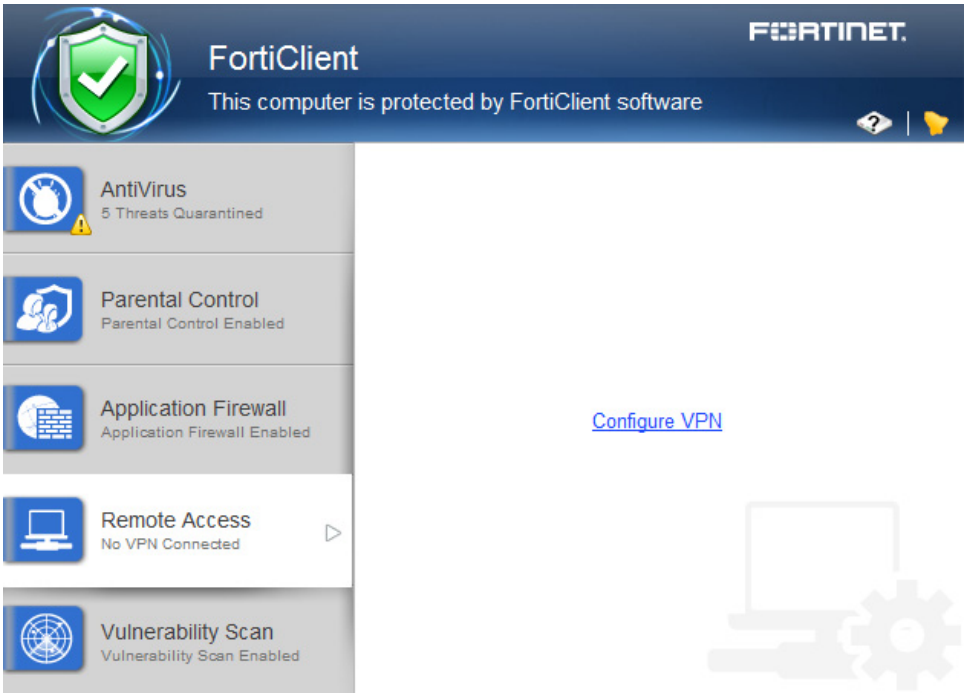
FortiClient v5.0 supports both IPsec and SSL-VPN connections to your network for remote access.

This section describes how to configure remote access.

Add a new connection

Select *Configure VPN* on the FortiClient dashboard to add a new VPN configuration.

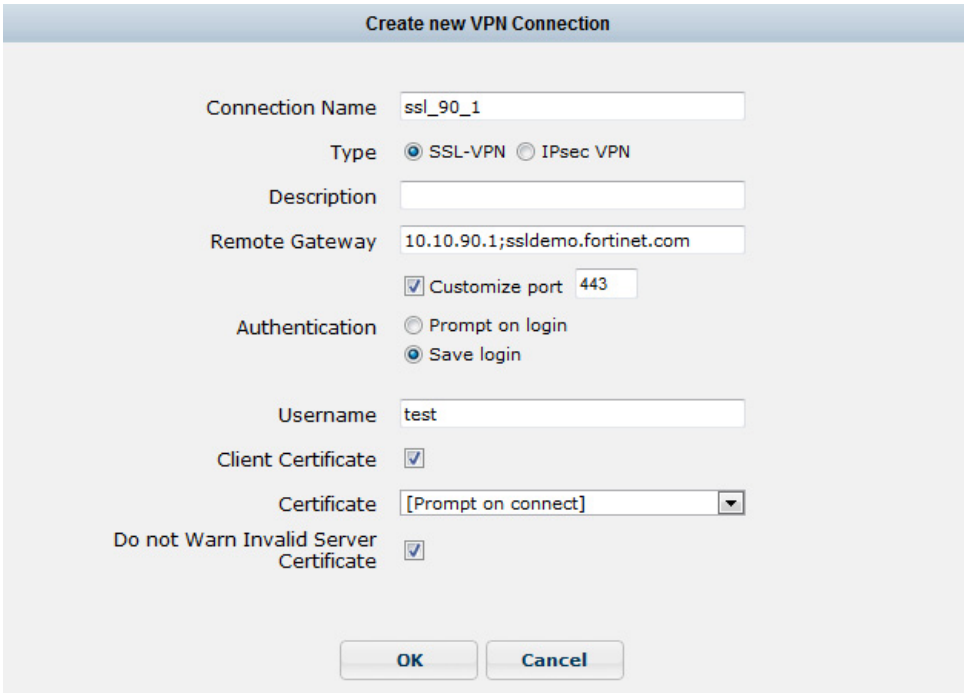
Figure 56: Configure a new VPN connection



Create a new SSL-VPN connection

To create a new SSL-VPN connection, select *Configure VPN* or use the drop-down menu on the dashboard. On this menu you can configure options outlined in the following figure and table.

Figure 57:SSL-VPN configuration options



Connection Name	Enter a name for the connection.
Type	Select SSL-VPN.
Description	Enter a description for the connection. (optional)
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
Port	Select to change the port. The default port is 443.
Authentication	Select to prompt on login, or save login.
Username	If you selected to save login, enter the username in the dialog box.
Client Certificate	Select to enable client certificates.
Certificate	Select the certificate option on the drop-down menu.
Do not warn Invalid Server Certificate	Select if you do not want to warned if the server presents an invalid certificate.

Create a new IPsec VPN connection

To create a new IPsec VPN connection, select *Configure VPN* or use the drop-down menu on the GUI. On this menu you can configure options outlined in the following figure and table.

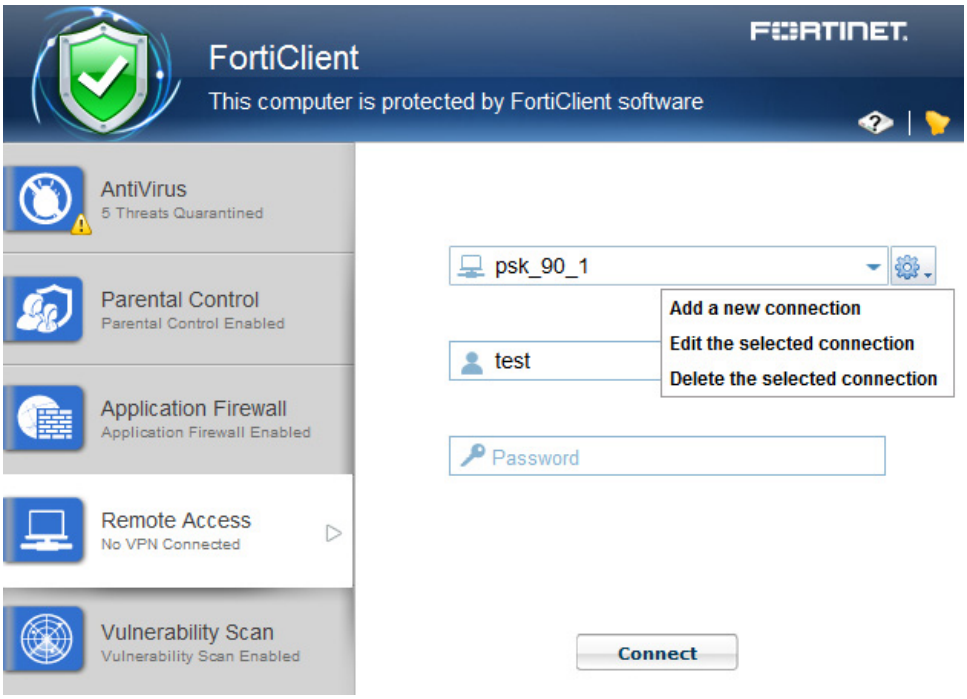
Figure 58:IPsec VPN configuration options

Connection Name	Enter a name for the connection.
Type	Select IPsec VPN.
Description	Enter a description for the connection. (optional)
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
Authentication Method	Select either *X.509 Certificate* or *Pre-shared Key* on the drop-down menu.
X.509 Certificate, Pre-shared Key	Select *X.509 Certificate* on the drop-down menu, or enter the pre-shared key in the dialog box. See Certificate Management for information on configuring certificate options.
Authentication (XAuth)	Select to prompt on login, save login, or disable.
Username	If you selected save login, enter the username in the dialog box.

Connect to a VPN

To connect to a VPN, select the name of the VPN from the drop-down menu. Enter your username, password, and select the *Connect* button.

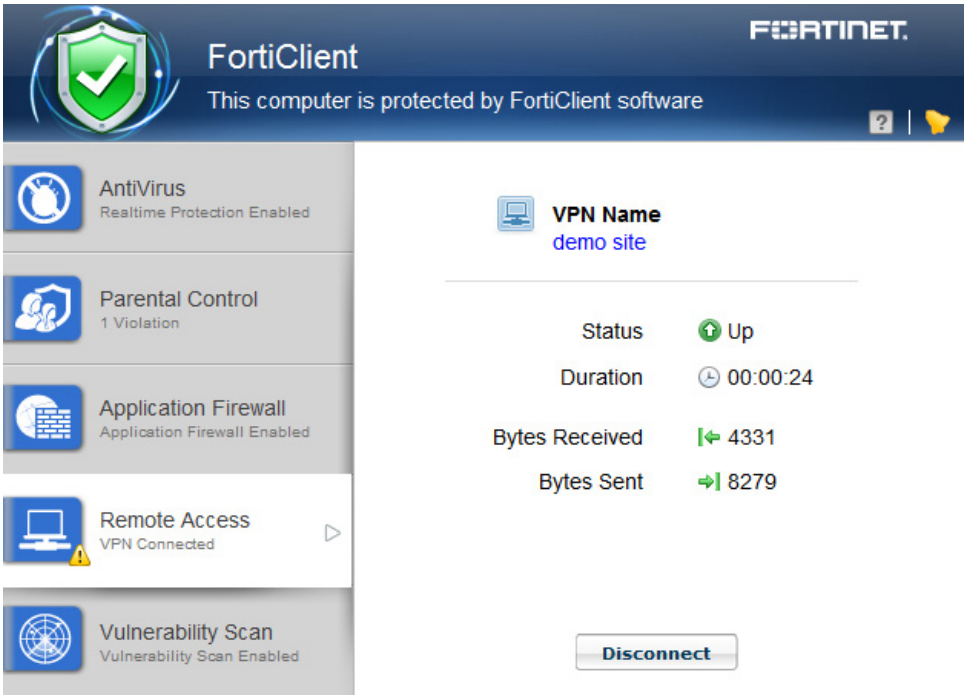
Figure 59: Connection options



You can also select to edit an existing VPN connection and delete an existing VPN connection using the drop-down menu.

When connected, the dashboard will display the connection status, duration, and other relevant information. You can now browse your remote network. Select the *Disconnect* button when you are ready to terminate the VPN session.

Figure 60:SSL-VPN connection established



Status	The status of the VPN connection.
Duration	The duration of the VPN connection.
Bytes Received	Bytes received through the VPN connection.
Bytes Sent	Bytes sent through the VPN connection.

Advanced features (Windows)

Connect VPN before logon (AD environments)

The VPN `<options>` tag holds global information controlling VPN states. The VPN will connect first, then logon to AD/Domain.

```
<forticlient_configuration>
  <vpn>
    <options>
      <show_vpn_before_logon>1</show_vpn_before_logon>
      <use_windows_credentials>1</use_windows_credentials>
    </options>
  </vpn>
</forticlient_configuration>
```

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
      <options>
      ...
      </options>
        <connections>
          <connection>
            <name>psk_90_1</name>
            <type>manual</type>
            <ike_settings>
            <prompt_certificate>0</prompt_certificate>
            <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61
                .143</server>
            <redundantsortmethod>1</redundantsortmethod>
            ...
        </ike_settings>
      </connection>
    </connections>
  </ipsecvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first on the list.

Priority based SSL-VPN connections

SSL-VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
  <vpn>
    <sslvpn>
      <options>
        <enabled>1</enabled>
        ...
      </options>
      <connections>
        <connection>
```

```
            <name>ssl_90_1</name>
            <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:44
                3</server>
            ...
          </connection>
        </connections>
      </sslvpn>
    </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL-VPN, all FortiGates must use the same TCP port.

Enabling VPN autoconnect

VPN auto connect uses the following XML tag:

```
<autoconnect_tunnel>ipsecdemo.fortinet.com</autoconnect_tunnel>
```

Inside:

```
<vpn>
  <options>
```

Save password is also needed because it is autoconnect:

```
<save_password>1</save_password>
```

Enabling VPN always up

VPN always up uses the following XML tag:

```
<keep_running>1</keep_running>
```

Inside:

```
<vpn>
  <connection>
```

Advanced features (Mac OS X)

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
      <options>
      ...
      </options>
        <connections>
          <connection>
            <name>psk_90_1</name>
            <type>manual</type>
            <ike_settings>
            <prompt_certificate>0</prompt_certificate>
            <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61
              .143</server>
            <redundantsortmethod>1</redundantsortmethod>
            ...
        </ike_settings>
      </connection>
    </connections>
  </ipsecvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first on the list.

Priority based SSL-VPN connections

SSL-VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
  <vpn>
    <sslvpn>
      <options>
        <enabled>1</enabled>
        ...
```

```
        </options>
        <connections>
          <connection>
            <name>ssl_90_1</name>
            <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:44
                3</server>
            ...
          </connection>
        </connections>
      </sslvpn>
    </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL-VPN, all FortiGates must use the same TCP port.

Enabling VPN autoconnect

VPN auto connect uses the following XML tag:

```
<autoconnect_tunnel>ssl 198 no cert</autoconnect_tunnel>
```

Enabling VPN always up

VPN always up uses the following XML tag:

```
<keep_running>1</keep_running>
```

VPN before logon is currently not supported in FortiClient v5.0 Patch Release 1 (Mac OS X).

VPN tunnel & script (Windows)

Feature overview

This feature supports auto running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in Mac OS X. They will be defined as part of a VPN tunnel configuration on FortiGate's XML format Endpoint Profile. The profile will be pushed down to FortiClient from FortiGate. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel will be executed.

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
  <script>
    <os>windows</os>
      <script>
        <script>
          <![CDATA[
net use x: \\192.168.10.3\ftpshare /user:Honey Boo Boo
md c:\test
copy x:\PDF\*.* c:\test
              ]]>
        </script>
      </script>
  </script>
</on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
  <script>
    <os>windows</os>
    <script>
      <script>
        <![CDATA[
net use x: /DELETE
          ]]>
</script>
      </script>
    </script>
</on_disconnect>
```

VPN tunnel & script (Mac OS X)

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
  <script>
    <os>mac</os>
    <script>
      /bin/mkdir /Volumes/installers
      /sbin/ping -c 4 192.168.1.147 >
           /Users/admin/Desktop/dropbox/p.txt
      /sbin/mount -t smbfs
           //kimberly:RigUpTown@ssldemo.fortinet.com/installer
```

```
            s /Volumes/installers/ >
            /Users/admin/Desktop/dropbox/m.txt
        /bin/mkdir /Users/admin/Desktop/dropbox/dir
        /bin/cp /Volumes/installers/*.log
            /Users/admin/Desktop/dropbox/dir/.
    </script>
  </script>
</on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
  <script>
    <os>mac</os>
    <script>
      /sbin/umount /Volumes/installers
      /bin/rm -fr /Users/admin/Desktop/dropbox/*
  </script>
  </script>
</on_disconnect>
```

For more information, see the *FortiClient v5.0 XML Reference* at the Fortinet Technical Documentation site, http://docs.fortinet.com.

Vulnerability Scan

Vulnerability Scan

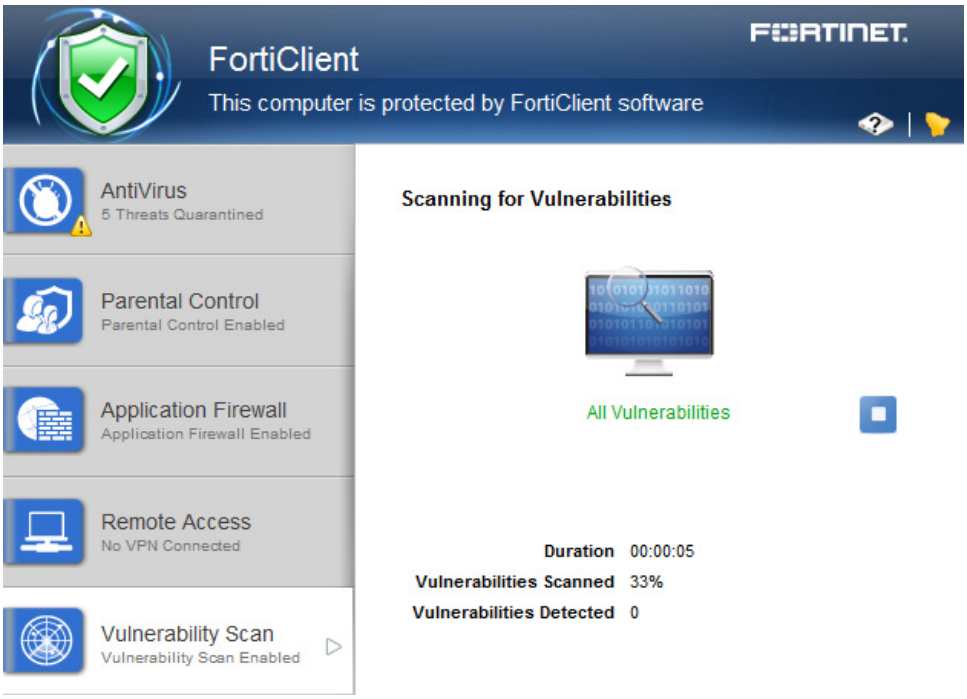
FortiClient v5.0 includes an Vulnerability Scan module to check your personal computer for known system vulnerabilities.

This section describes how to enable Vulnerability Scan, and configuration options.

Scan Now

To perform a vulnerability scan, select the *Scan Now* button on the FortiClient dashboard. FortiClient will scan your personal computer for known vulnerabilities. The dashboard notes the date of the last scan above the button.

Figure 61: Vulnerability scan in progress



Update Now

Select the *Update Now* button on the FortiClient dashboard to update the vulnerability signature.

View Vulnerabilities

When the scan is complete, FortiClient will display the number of vulnerabilities found on the dashboard. Select the *Found* link to view a list of vulnerabilities detected on your system.

Figure 62: Vulnerabilities detected page

Vulnerabilities Detected in the Last 30 Days

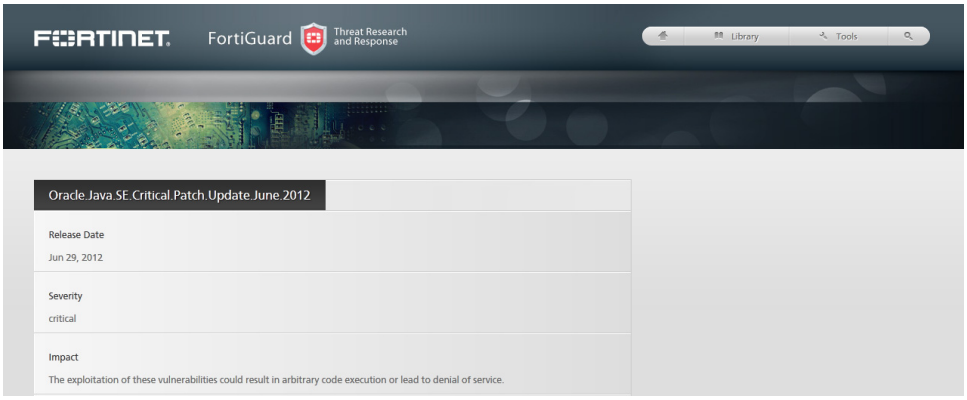
Vulnerability Name	Severity	Details	Time
Most Recent Scan			
1 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-24	Critical	33877	24/12/2012 2:35:21 PM
2 MS.VS.Active.Template.Library.Remote.Code.Execution	Critical	20531	24/12/2012 2:35:21 PM
3 Oracle.Java.SE.Critical.Patch.Update.October.2012	Critical	33716	24/12/2012 2:35:21 PM
4 Oracle.Java.SE.Critical.Patch.Update.Advisory.February.2012	Critical	32669	24/12/2012 2:35:21 PM
5 Oracle.Java.SE.Critical.Patch.Update.February.2011	Critical	27928	24/12/2012 2:35:21 PM
6 Oracle.Java.SE.Critical.Patch.Update.June.2011	Critical	30899	24/12/2012 2:35:21 PM
7 Oracle.Java.Runtime.True.Type.Font.IDEF.Opcode.Buffer.Ove...	Critical	31444	24/12/2012 2:35:21 PM
8 Oracle.Java.Runtime.Environment.Memory.Corruption.Vulnera...	Critical	33599	24/12/2012 2:35:21 PM
9 Oracle.Java.MixerSequence.Array.Index.Remote.Code.Execut...	Critical	30551	24/12/2012 2:35:21 PM
10 Oracle.Java.FileDialog.Show.Buffer.Overflow	Critical	28761	24/12/2012 2:35:21 PM
11 Oracle.Java.SE.Critical.Patch.Update.June.2012	Critical	32430	24/12/2012 2:35:21 PM
12 Microsoft.XML.Core.Services.Remote.Code.Execution.Vulner...	Critical	32958	24/12/2012 2:35:21 PM
13 MS.Windows.Unauthorized.Digital.Certificates.Spoofing.KB2...	Critical	32685	24/12/2012 2:35:21 PM
14 Apple.Safari.Multiple.Vulnerabilities.APPLE-SA-2012-11-01-2	Critical	33927	24/12/2012 2:35:21 PM
15 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-14	Critical	32255	24/12/2012 2:35:21 PM
16 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-19	Critical	33028	24/12/2012 2:35:21 PM
17 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-22	Critical	33582	24/12/2012 2:35:21 PM

Close Clear

Vulnerability Name	The name of the vulnerability
Severity	The severity level assigned to the vulnerability; Critical, High, Medium, Low, Info.
Details	FortiClient vulnerability scan lists a Bugtraq (BID) number under the details column. You can select the BID to view details of the vulnerability on the FortiGuard site, or search the web using this BID number.
Time	The date and time that the vulnerability was detected.
Close	Close the window and return to the FortiClient dashboard.
Clear	Clear the Vulnerability Scan results.

Select the *Details* ID number from the list to view information on the selected vulnerability on the FortiGuard site. The site details the release date, severity, impact, description, affected products, and recommended actions.

Figure 63: FortiGuard site details



Vulnerability Scan logging

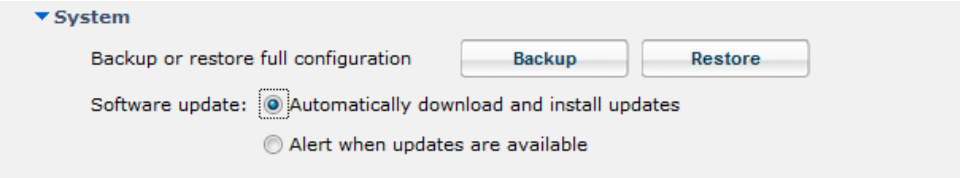
To configure Vulnerability Scan logging, select *File* on the toolbar, and *Settings* on the drop-down menu. Select *Logging* to view the drop-down menu. Select *Vulnerability Scan* on the logging menu to enable logging for this module.

Settings

Backup or restore full configuration

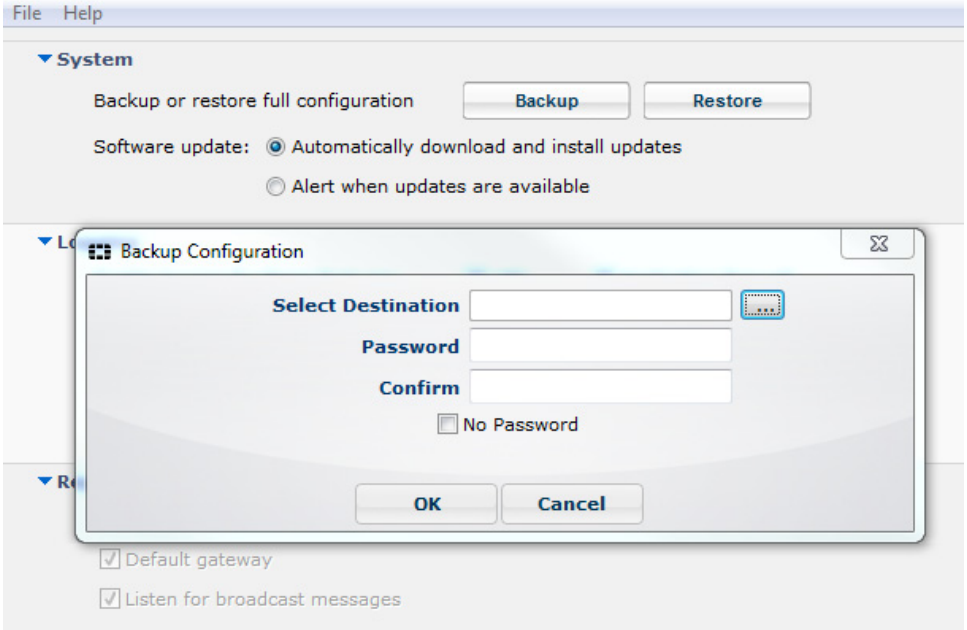
To backup or restore the full configuration file select *File* on the toolbar and *Settings* on the drop-down menu. Select *System* to view the drop-down menu. On this menu you can perform a backup or restore a full configuration file.

Figure 64: Backup and restore options



When performing a backup you can select the file destination and save the file in an unencrypted or encrypted format.

Figure 65: Backup file options



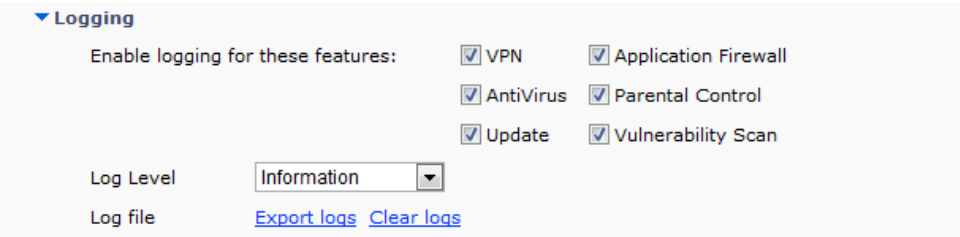
Logging

To configure logging, select *File* on the toolbar and *Settings* on the drop-down menu. Select *Logging* to view the drop-down menu. On this menu you can configure logging for the following features:

- VPN
- Antivirus
- Update
- Application Firewall
- Parental Control
- Vulnerability Scan

You can specify the logging level and select to export logs or clear logs.

Figure 66: Logging options

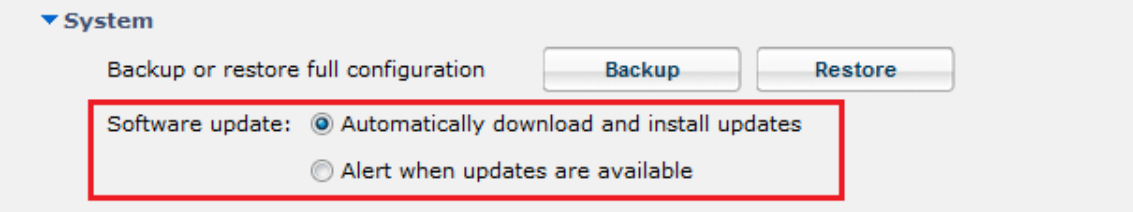


Logging Level	Description
Emergency	The system becomes unstable.
Alert	Immediate action is required.
Critical	Functionality is affected.
Error	An error condition exists and functionality could be affected.
Warning	Functionality could be affected.
Notice	Information about normal events.
Information	General information about system operations.
Debug	Debug FortiClient.

Updates

To configure updates, select *File* on the toolbar and *Settings* on the drop-down menu. Select *System* to view the drop-down menu. On this menu you can configure the behavior of FortiClient when a new software version is available on the FortiGuard Distribution Servers (FDS).

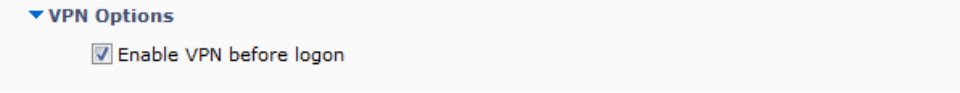
Figure 67: Update options



VPN options

To configure VPN options, select *File* on the toolbar and *Settings* on the drop-down menu. Select *VPN Options* to view the drop-down menu. On this menu you can configure to enable VPN before logon.

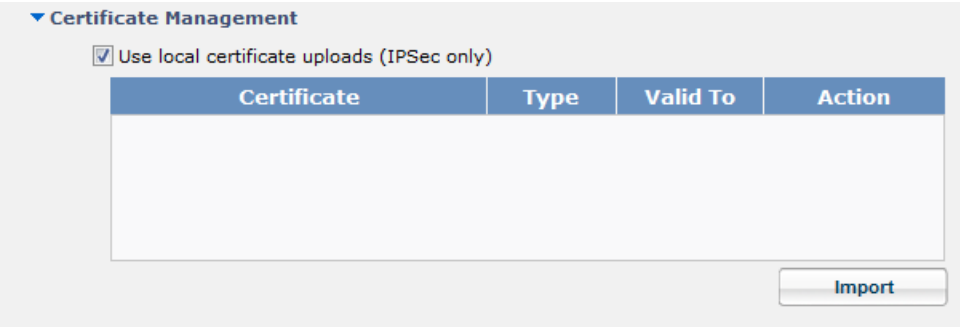
Figure 68:VPN options



Certificate Management

To configure VPN certificates, select *File* on the toolbar and *Settings* on the drop-down menu. Select *Certificate Management* to view the drop-down menu. On this menu you can configure IPsec VPN to use local certificates and import certificates to FortiClient.

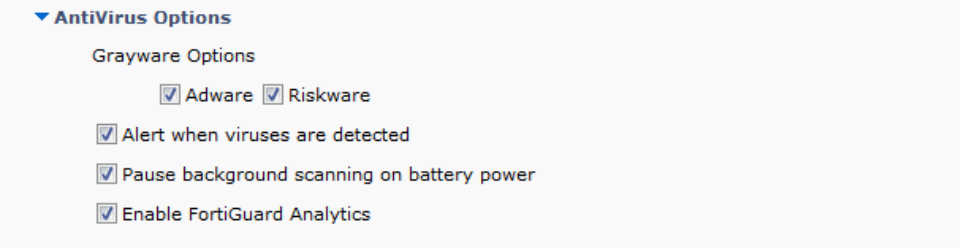
Figure 69: Certificate options



Antivirus options

To configure antivirus options, select *File* on the toolbar, and *Settings* on the drop-down menu. Select *AntiVirus Options* to view the drop-down menu. On this menu you can configure grayware options and the behavior of FortiClient when a virus is detected.

Figure 70: Antivirus options

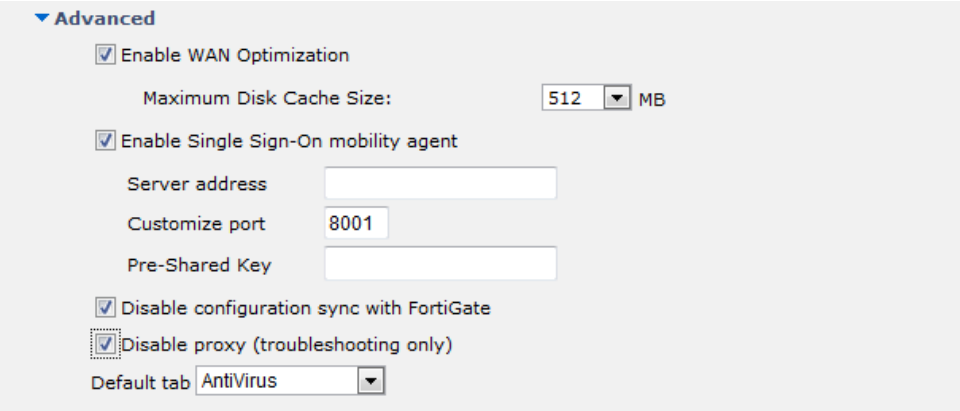


Grayware Options	Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge.
Adware	Select to enable adware detection and quarantine during the antivirus scan.
Riskware	Select to enable riskware detection and quarantine during the antivirus scan.
Alert when viruses are detected	Select to display notification message window when a virus is detected.
Pause background scanning on battery power	Select to pause background scanning when on battery power.
Enable FortiGuard Analytics	Select to automatically send suspicious files to the FortiGuard Network for analysis.

Advanced options

To configure advanced options, select *File* on the toolbar, and *Settings* on the drop-down menu. Select *Advanced* to view the drop-down menu. On this menu you can configure WAN Optimization, Single Sign-On, configuration sync with FortiGate, disable proxy, and the default tab when FortiClient is started.

Figure 71: Advanced options



Advanced	
Enable WAN Optimization	Select to enable WAN Optimization. You should enable only if you have a FortiGate device and your FortiGate is configured for WAN Optimization.
Maximum Disk Cache Size	Select to configure the maximum disk cache size. The default value is 512MB.
Enable Single Sign-On mobility agent	Select to enable Single Sign-On Mobility Agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device.
Server address	Enter the FortiAuthenticator IP address.
Customize port	Enter the port number. The default port is 8001.
Pre-Shared Key	Enter the pre-shared key. The pre-shared key should match the key configured on the FortiAuthenticator.
Disable configuration sync with FortiGate	Select to disable configuration synchronization with FortiGate.
Disable proxy (troubleshooting only)	Select to disable proxy when troubleshooting FortiClient.
Default tab	Select the default tab to be displayed when opening FortiClient.

Single Sign-On Mobility Agent

The FortiClient Single Sign-On Mobility Agent acts as a client that updates with FortiAuthenticator with user logon and network information.

FortiClient/FortiAuthenticator Protocol

The FortiAuthenticator listens on a configurable TCP port. FortiClient connects to FortiAuthenticator using TLS/SSL with two-way certificate authentication. The FortiClient sends a logon packet to FortiAuthenticator, which replies with an acknowledgement packet.

FortiClient/FortiAuthenticator communication requires the following:

- The IP address should be unique in the entire network.
- The FortiAuthenticator should be accessible from clients in all locations.
- The FortiAuthenticator should be accessible by all FortiGates.

FortiClient Single Sign-On Mobility Agent requires a FortiAuthenticator running v2.0.0 GA build 0006 or later. Enter the FortiAuthenticator (server) IP address, port number, and the pre-shared key configured on the FortiAuthenticator.

Enable Single Sign-On Mobility Agent on FortiClient

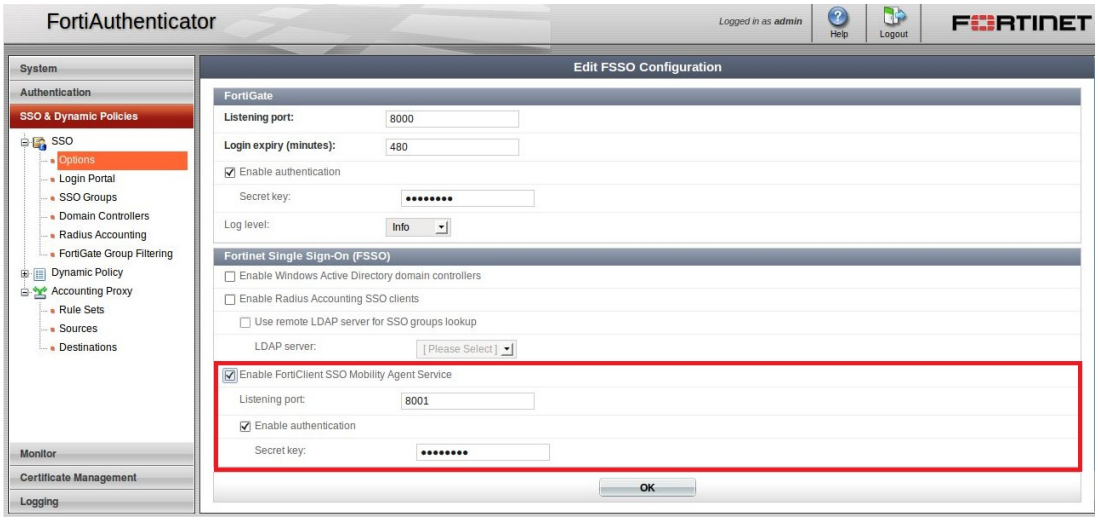
1. Select *File* on the toolbar and *Settings* on the drop-down menu.
2. Select *Advanced* to view the drop-down menu.
3. Select to *Enable Single Sign-On mobility agent*.

4. Enter the FortiAuthenticator server address and the pre-shared key.

Enable FortiClient SSO Mobility Agent Service on the FortiAuthenticator

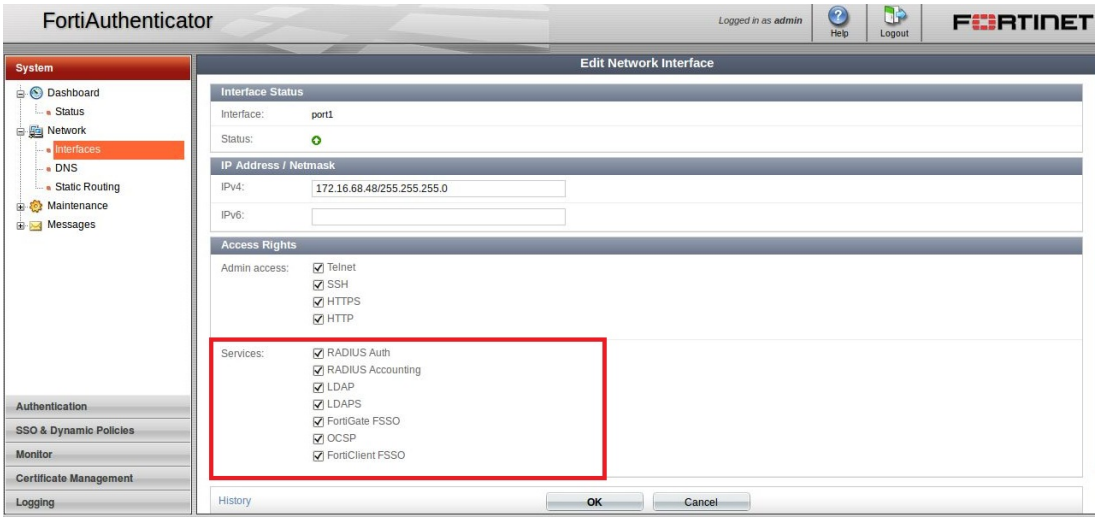
1. Select *SSO & Dynamic Policies* > *SSO* > *Options*.
2. Select *Enable FortiClient SSO Mobility Agent Service* and a TCP port value for the listening port.
3. Select *Enable authentication* and enter a secret-key value.

Figure 72: FortiAuthenticator configuration



4. To enable FortiClient FSSO services on the interface, select *System* > *Network* > *Interface*. select *Edit* to edit the network interface, select *FortiClient FSSO* to enable.

Figure 73: Enable services

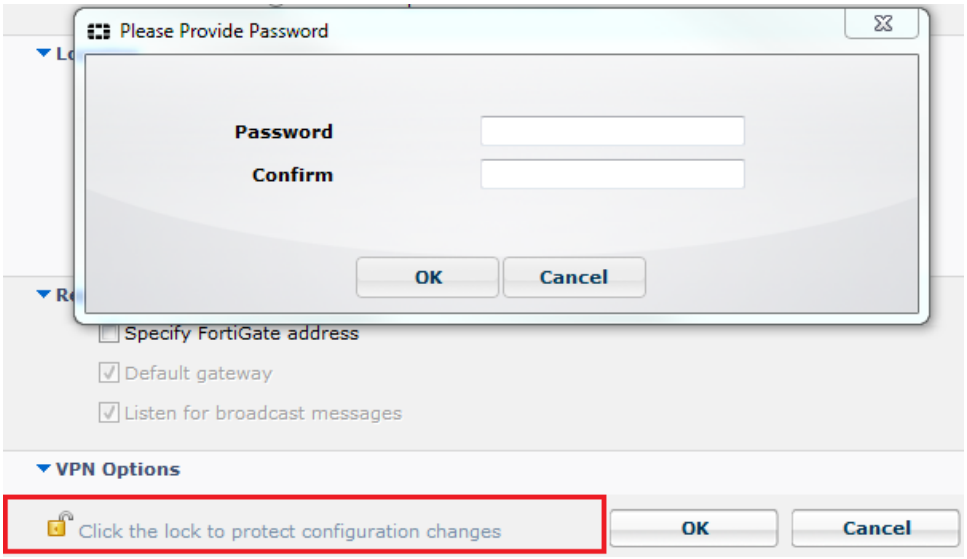


To enable the FortiClient SSO Mobility Agent Service on the FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. For more information, see the *FortiAuthenticator v2.0 Administration Guide* at http://docs.fortinet.com. For information on purchasing a FortiClient license for FortiAuthenticator, please contact your authorized Fortinet reseller.

Configuration lock

To prevent unauthorized changes to the FortiClient configuration, select the lock icon located at the bottom left of the *Settings* page. You will be prompted to enter and confirm a password. When the configuration is locked, configuration changes are restricted and FortiClient cannot be shut down or uninstalled.

Figure 74: Configuration lock



When the configuration is locked you can perform the following actions:

- Antivirus
  - Complete an antivirus scan, view threats found, and view logs
  - Select *Update Now* to update signatures
- Parental Control
  - View violations
- Application Firewall
  - View applications blocked
- Remote Access
  - Configure, edit, or delete an IPsec VPN or SSL-VPN connection
  - Connect to a VPN connection
- Vulnerability Scan
  - Complete a vulnerability scan of the system
  - View vulnerabilities found
- Register and unregister FortiClient for Endpoint Control
- Settings
  - Export FortiClient logs
  - Backup the FortiClient configuration

To perform configuration changes or to shut down FortiClient, select the lock icon and enter the password used to lock the configuration.

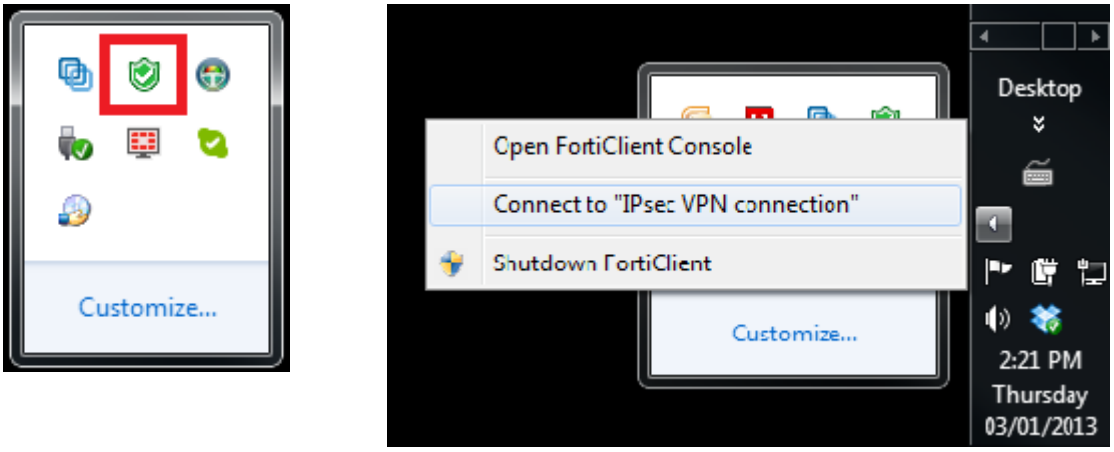
FortiTray

When FortiClient is running on your system, you can select the FortiTray icon on the Windows system tray to perform various actions. The FortiTray icon is available in the system tray even when the FortiClient dashboard is closed.

- Default menu options
  - Open FortiClient console
  - Shutdown FortiClient
- Dynamic menu options depending on configuration
  - Connect to a configured IPsec VPN or SSL-VPN connection
  - Display the antivirus scan window (if a scheduled scan is currently running)
  - Display the Vulnerability scan window (if a vulnerability scan is running)

If you hover the mouse cursor over the FortiTray icon, you will receive various notifications including the version, AV signature, and AV engine.

Figure 75: System tray icon

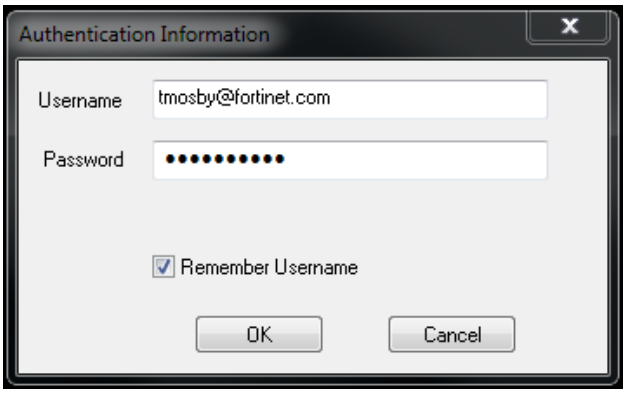


When the configuration is locked, the option to shut down FortiClient from FortiTray is greyed out.

Connect to a VPN connection

To connect to a VPN connection from FortiTray, select the Windows System Tray and right click on the FortiTray icon. Select the connection you wish to connect to, enter your username and password in the authentication window, and select *OK* to connect.

Figure 76: Authentication window



Index

A

antivirus
- custom scan 36, 38
- enable or disable 35
- exclusion list 40
- full scan 36, 38
- logging 41
- notifications 35
- perform on-demand scanning 36
- quick scan 36, 38
- schedule a scan 38
- update now 37
- view quarantined threats 39

application firewall
- application firewall rules 46
- enable or disable 45
- logging 47
- view applications blocked 45

E

Enable Registration Key for FortiClient 34

F

forticlient
- licensing 7

FortiClient Endpoint Registration 34
FortiTray 69

G

grayware 10

I

installation
- EULA 12, 15
- forticlient 12, 15
- language support 9
- minimum system requirements 8
- setup wizard 12, 15
- supported operating systems 8

L

licensing 7

M

MSI
- custom MSI installation 19
- FortiClient Configurator 18
- Microsoft Active Directory 19
- Microsoft System Center Configuration Manager 20

R

registration key 34
remembered FortiGates 32

S

settings
- advanced options 65
- antivirus 64
- backup or restore the full configuration file 62
- certificate management 64
- logging 63
- SSO mobility agent 66
- updates 63
- VPN options 64

V

vulnerability scan
- Bugtraq ID 60
- logging 61
- perform a vulnerability scan 59
- update now 59
- view scan results 60

X

XML
- always up 54
- autoconnect 54
- connect VPN before logon 52
- create a redundant IPsec VPN 57
- priority based SSL-VPN connections 53, 55